

عصر الفرص الجديدة

الحكومة الذكية

عباس بدران

www.egovconcepts.com

عصر الفرص الجديدة

الحكومة الذكية

عصر الفرص الجديدة

الحكومة الذكية

عباس بدران



الدار العربية للعلوم ناشرون ش.م.ل
Arab Scientific Publishers, Inc. S.A.L

بسم الله الرحمن الرحيم

الطبعة الأولى:

1435 هـ - 2014 م

ردمك 978-614-01-1188-2



عين التينة، شارع المفتي توفيق خالد، بناية الريم

هاتف: 786233 - 785108 - 785107 (1-961+)

ص.ب: 5574-13 شوران - بيروت 2050-1102 - لبنان

فاكس: 786230 (1-961+) - البريد الإلكتروني: asp@asp.com.lb

الموقع على شبكة الإنترنت: http://www.asp.com.lb

التنضيد وفرز الألوان: **أبجد غرافيكس**، بيروت - هاتف 785107 (9611+)

الطباعة: **مطابع الدار العربية للعلوم**، بيروت - هاتف 786233 (9611+)

الإهداء

إلى الشباب العربي من المحيط إلى الخليج

وكل من يكتب باللغة العربية

بالرغم من التحديات التقنية واللغوية

وابتعاد الكثيرين عن اللغة الأجمل

الحكومة الذكية:

عصر الفرص الجديدة

في هذا الكتاب يقوم المؤلف بتعريف الحكومة الذكية ويشرح أهم العوامل التي تدفع الحكومات حول العالم بإتجاه توطين أدوات الذكاء والمعرفة، كما يخصص فصلاً كاملاً عن الأمن الذكي في الحكومة حتى لا تقع تلك الحكومات في خطر الإنغماس التكنولوجي الغير محسوب العواقب. ويستفيد من الكتاب أصحاب القرار في الحكومات ومدراء المعلوماتية فيها وكل من يعمل في تطوير تطبيقات حكومية ذكية.

إقرأ في هذا الكتاب:

- ماذا يميز نموذج الحكومة الذكية عن غيره؟
- ما هي الحوسبة السحابية وكيف تستفيد منها الحكومة؟
- هل تستطيع الحكومة أن تعزل نفسها عن الحراك الإجتماعي الإلكتروني؟
- الخدمات الحكومية الجوّالة ومعايير تأمينها
- لماذا لم يعد الأمن التقليدي كافياً لدرء المخاطر والتهديدات؟
- تعرف على بعض التطبيقات الحكومية الذكية

فهرس المحتويات

فهرس النماذج

فهرس الجداول

مقدمة الكتاب

مضت عشر سنوات منذ أن نشرت كتاب الحكومة الإلكترونية من الإستراتيجية إلى التطبيق عام 2004 تغيرت خلالها التكنولوجيا بطريقة مثيرة جداً حتى قبل أن تستوعب بعض الحكومات المحلية أهمية تطوير نماذجها من أجل البقاء. وقد ذكرت في خلاصة الكتاب المذكور العبارة التالية: "لقد إنتقل الإعلام إلى الفضاء بينما بقيت الحكومة على الأرض" حيث اتّسمت تلك الفترة بهيمنة وسائل الإعلام الفضائية الخارجية على الإعلام المحلي مما أدى بالمواطن إلى أن يستقي معلوماته من الإعلام الفضائي بدلاً من إعلام الدولة او الحكومة المحلي. لم تستطع الحكومات في تلك الفترة أن تتلمس خطورة ان تبقى على الحياد ففقدت الكثير من الحكومات العربية السيطرة على مجتمعاتها إلى أن ظهرت بعض الثورات مدعومةً بأفكار تنتقل بسرعة الضوء عبر الألياف والشبكات الإجتماعية الإلكترونية وتجد لها صدى في فئات الشباب في مختلف البلدان العربية. واليوم أيضاً تضع التكنولوجيا الحديثة والذكية تحديات جمّة أمام الحكومات إذا لم تستطع الرد عليها بجدارة فسوف يأتي من يملأ الفراغ لدى المواطن وتصبح الحكومة عبارة عن فراغ إجتماعي وإنفصال عن واقع وحياة مواطنيها وهيكل إداري يكاد يهترئ وأنظمة وإجراءات تعيق حركة الإزدهار والنموّ أكثر مما تساعد لأن جمهورها وشبابها سوف يكونوا قد إنتقلوا إلى واقع آخر.

وكما في كل التحديات تكمن الفرص، كذلك تتراءى الكثير من الفرص التطويرية والإستثمارية في الأفق وما على الحكومة إلا التموضع جيداً من أجل إقتناصها، ويبدأ تموضع الحكومة بتطوير كوادرها وقادتها ومسؤوليها وتشجيع بيئة الإبداع بين مواطنيها وتحديث سلة خدماتها وإستغلال التطورات التكنولوجية وبدء ورشة عمل تنموية من أجل الإنتقال إلى إقتصاد المعرفة بثقة وثبات ووضوح في الرؤية.

إن الحكومة الذكية هي التطور الطبيعي للحكومة الإلكترونية نظراً لظهور وتغلغل التكنولوجيا والأجهزة الذكية بين أيدي معظم المواطنين، ويسرني أن أقدم للحكومات العربية ومواطنيها على سبيل السواء هذا الكتاب التمهيدي حول ملامح وآليات تلك الحكومة.

الإتصال بالمؤلف

إيكونسبت الإستشارية - مركز دراسات الحكومة الالكترونية

بيروت - لبنان

بريد إلكتروني abbas.badran@gmail.com

موقع الإنترنت للدراسات www.egovconcepts.com

موقع الإنترنت للمؤسسة الإستشارية www.econcepts.me

يقدم المركز دورات تدريبية متخصصة للمستوى الإستراتيجي والتنفيذي حول مفاهيم الحكومة الالكترونية والذكية وكذلك دورات تطبيقية وبرمجية حول إنشاء مواقع الإنترنت الديناميكية وتطبيقات الهاتف الجوّال وإدارة البنية التحتية لمراكز الداتا والعديد من الدورات وورش العمل عن لغات البرمجة المشهورة.

عصر الفرص الجديدة

شهدت السنوات العشر الماضية ثورة في تطبيقات وتكنولوجيا الأجهزة المحمولة وقد ذكرت بعض الإحصاءات الصادرة عن شركات عالمية ومنها شركة "سوبر مونيتورنغ" أن ما يقارب من 50 % من سكان العالم يستخدمون أجهزة الهاتف الذكية ومعظم هؤلاء يتصفحون الإنترنت من خلال تلك الأجهزة.

- 24 مليار جهاز متنوع متصل بالإنترنت بحلول العام 2020
- على المستوى العالمي 1 من كل 5 أشخاص يحمل هاتف ذكي بنهاية عام 2013
- حوالي 2 مليار ونصف مستخدم للإنترنت حول العالم أي حوالي ثلث سكان الأرض
- نظام الرسائل الجوالة القصيرة (SMS) يترنح تحت ضربات الواتس أب (Whatsapp) والذي بلغ عدد مستخدميه حوالي 400 مليون.

وبموازة أجهزة الهاتف الشخصية، قامت الأجهزة اللوحية الصغيرة (iPad, Tablet) بإختراق المؤسسات عبر تطبيقات متنوعة في قطاع الصحة والوقاية وقطاع النفط والغاز والادارة الداخلية والأجهزة الحكومية وصولاً إلى المكتبات العامة والنوادي الصحية والفنادق.

وقد كان لفتح الأنظمة البرمجية للنظام أندرويد وفـتح واجهـة التطبيقات (iOS SDK) للنظام الخاص بأجهزة الآي فون الأثر الكـبير في ظهور الآلاف من التطبيقات الجوالة في فترة زمنية صـغيرة جـداً مقارنة بالفترة التي تطورت فيها تطبيقات الوب، وفي نفـس الوقـت كانت تكنولوجيا الحوسبة السحابية (Cloud Computing) تتطـور على قدم وساق مما أدى بطريقة غير مباشرة إلى تـأمين بنيـة تحتيـة حاسوبية مطّاطة وتحت الطلب للتطبيقات الجوالـة بحيـث تسـتطيع المؤسسات أن تنطلق من تطبيق جوّال يخدم عشرات المسـتخدمين إلى نفس التطبيق بقدرة تشغيلية تخدم ملايين المستخدمين وكل ذلك عـبر السحابة الحاسوبية التي يتم حساب كلفتها حسب كمية الاسـتخدام الفعلي للمعالجات ووسائط التخزين وناقلات الداتا.

لم يتوقف التطور عند هذا الحد، بـل إنتشـرت في الفضـاء الالكتروني مجموعة من "الأدوات أو الأشياء" الالكترونية الخدميـة على شكل أجهزة استشعار تقـيس المنـاخ ومعـدلات الصـحة الشخصية والتغييرات البيئية والمناخية وغيرها من الأمور، إنتشـرت تلك الأشياء الالكترونية المرتبطة بالإنترنت من أجل تشـكيل مـا سوف نطلق عليه "إنترنت الأشياء" (Internet of Things) والـتي تهدف إلى تجميع الداتا بشكل أوتوماتيكي مـن مصـادر مختلفـة وإرسالها إلى خودام وسيرفيرات التحليل والدراسة من أجل توظيف معلوماتها في مجالات الوقاية الصحية وزيـادة الإنتـاج وتخفـيض الأكلاف التشغيلية.

إنه عصر الفرص الجديدة ولا يمكن للحكومة، وهـي اللاعـب الأكبر والأساسي في المجتمع، أن تبقى متفرجة على كل تلك التطورات والفرص من دون محاولة استثمارها من أجل النهوض بمستوى خدماتها

العامة بعد أن وصلت إلى مرحلة الاستقرار (Plateau) على جبهة تطبيقات الوب الكلاسيكية.

وكعادها فقد تلقفت دولة الامارات العربية المتحدة هذا التغيير بسرعة وردت عليه بإطلاق مبادرة الحكومة الذكية والتي هي إمتداد طبيعي لمشروع الحكومة الالكترونية الذي بلغ مداه في هذه الدولة. وقد أعلنت دولة الامارات العربية المتحدة أن هدفها هو توصيل الخدمة العامة الحكومية على إختلافها إلى أيدي المستخدمين مباشرة من خلال أجهزهم الجوالة في مشهد إتصالي مع المواطن لم نرى له مثيلاً من قبل: أن تكون الحكومة بهذا القرب من المواطن! أن تكون في جيبة المواطن.

الحكومة الذكية

"الأذكياء هم القادرون على التكيّف مع التغيير"

ستيفن هوكينغ

بخلاف الإعتقاد الشائع بأن الحكومة الذكية هي فقط مجموعة من التطبيقات الالكترونية على الأجهزة الجوالة الذكية، نحن نعتقد بأن الحكومة الذكية هي التطور الطبيعي لنموذج الحكومة الالكترونية الذي عايشناه خلال العقد الماضي، وفي الوقت الذي كانت الحكومة الالكترونية تسعى، بشكل عام، إلى تظهير الخدمات العامة الحكومية على الإنترنت من خلال تطبيقات الوب والبوابات الالكترونية وصياغتها بطريقة عادةً ما عكست الأحداث الحياتية للمواطن وسلّة خدمات الأعمال (Life Events & Business Episodes)، تأتي الحكومة الذكية وتطبيقاتها لكي تكمل ما تم بناؤه والاستثمار فيه عبر الاقتراب أكثر من المواطن من جهة، والتفاعل المباشر والمتزامن مع الداتا المنتشرة في المجتمع ومكوناته الإقتصادية والإجتماعية والأمنية من جهة أخرى. وقد تطورت أدوات وأجهزة الاستشعار الذكية (Smart Sensors) والتي ترتبط بالإنترنت مثل كاميرات المراقبة الأمنية في المدن وأجهزة إستشعار المناخ وأجهزة قياس إستهلاك الطاقة والكهرباء المرتبطة بشبكة إنترنت الحكومة، وغيرها من الأدوات الاستشعارية الذكية وساعدت في تطوير بيئة إلكترونية جديدة من الممكن أن تستفيد منها الحكومة في تشغيل

وصيانة خدماتها بطريقة أكثر فعالية وأقل كلفة وأقل عرضة لحصول الأخطاء البشرية أو التجاوزات الإدارية.

ويحتوي الجدول التالي على مقارنة عامة بين نماذج الحكومة التي تطورت وصولاً إلى الحكومة الذكية:

	الحكومة الكلاسيكية	الحكومة الالكترونية	الحكومة الذكية
محور النشاط	متمحورة حول الادارة العامة والوزارات.	متمحورة حول الخدمات العامة بغض النظر عن الادارة التي تقدمها.	متمحورة حول الفرد بشخصه والذي يحمل سلة خدماته ومعاملاته مع الحكومة في جيبه من خلال جواله.
وسيلة الاتصال الرئيسية	أدوات الاتصال التقليدية	البوابات الالكترونية والمواقع	التطبيقات الجوالة والشبكات الاجتماعية
الداتا الحكومية	الداتا بمختلف أنواعها غير متوفرة للجمهور	جزء من الداتا الحكومية متوفر عبر المواقع	عصر الداتا الضخمة المفتوحة Big Data
نموذج الحوسبة	الجهاز الخادم المركزي والطرفيات Mainframe	أجهزة الخادم – الزبون Client-Server	الحوسبة السحابية Cloud Computing
تحصيل وإدخال الداتا	إدخال يدوي من الورق والاستمارات	الورقيات والنماذج الالكترونية عبر المواقع الحكومية	الورقيات، النماذج الالكترونية، وداتا أجهزة الاستشعار الذكية وعبر أنظمة الباركود والكيو آر(QR code)

جدول 1: المقارنة بين نماذج الحكومات

وسوف تؤدي التطورات الجديدة إلى إجــراء الكــثير مــن التعديلات على نماذج الحكومة الالكترونية ومنها إدخال تحــديثات مناسبة علــى الإطــار التــوافقي لــداتا الحكومــة الالكترونيــة (Government Interoperability Framework) حــتى تــتلاءم مصادر ونسق الداتا الجديدة مع الأنظمة الخلفية للحكومة.

ومن أجل أن تتحول الحكومة الالكترونية إلى حكومة ذكية ســوف يتم العمل على عدة جبهات تقنية وإدارية وتشريعية في آن معاً ونذكر منها:

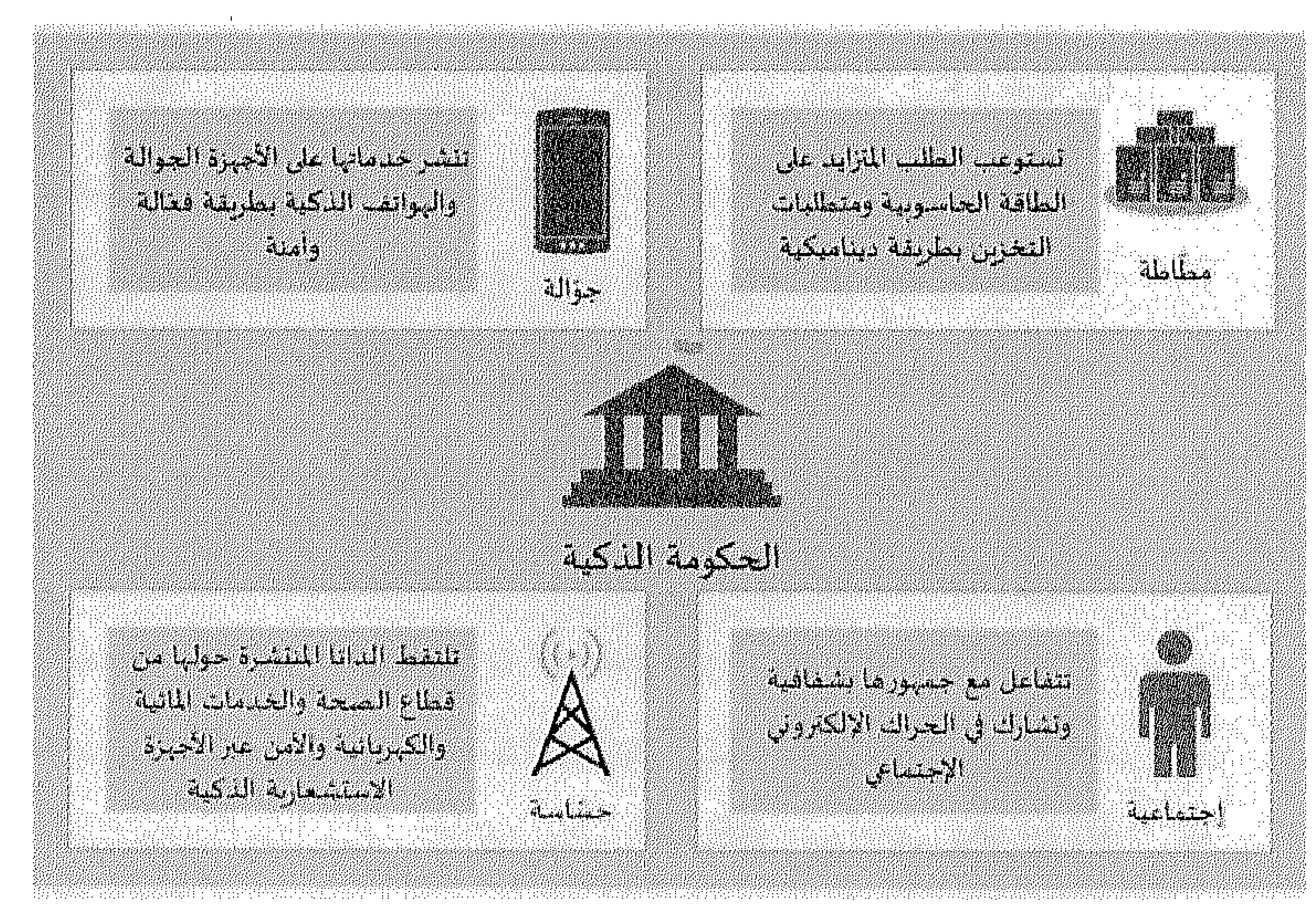
- إنشاء إطار عمل الخدمات الحكومية الذكية على الهواتــف الجوالة وكيفية تجميعها وتظهيرها بشكل يخدم الأفراد. وقد تكون الخدمات الحكومية الذكية مقدمة من خلال تطبيــق حكومي موحّد تكون الخدمة العامة فيه عنصراً خدمياً يــتم إضافته أو إزالته إلى ذلك التطبيق الضخم أو تعمد الحكومة المركزية إلى نشر توجيهات وإرشادات عامة حول كيفيــة تطوير الخدمات والتكنولوجيا المفضّلة لديها وكيفية التصميم ومحتويات الخدمة وكيفية تأمين وحماية الخدمة (أمن وسرية المعلومات) ثم تترك المجال للأجهزة والوزارات المختلفة مــن أجل أن يقوموا داخلياً بتطوير الخدمات الحكومية الذكيــة الخاصة بهم.
- تطوير إرشادات وقوالب خاصة بالتطبيقات الذكية (Smart Government Apps Guidelines). وقد قامت معظــم الحكومات بتطوير هذه الإرشادات الخاصة بــإطلاق مواقــع إنترنت حكومية ولكن حتى الآن لم تقم تلك الحكومات بنفس العمل على مستوى التطبيقات الذكية علماً ان وقت تفاعــل المواطن مع جهازه الجوال يتجاوز بكثير الوقت الذي يستهلكه

ذلك المواطن بتفاعله مع المتصفحات على الأجهزة المكتبية.

- العمل على فتح داتا الحكومة الضخمة (Government Big Data) من أجل تشجيع إطلاق التطبيقات الذكية حولها من قبل المبرمجين في المجتمع. ومثال على ذلك أن تفتح الحكومة داتا المعاملات التجارية والاقتصادية وداتا وسائل النقل والمواصلات وداتا الاستيراد والتصدير بشكلها الخام ويأتي من يبرمج تطبيقات ذكية على الهواتف من أجل خدمة التجار وتزويدهم بمعلومات يستفيدون منها في تجارتهم مع شركاء تجاريين في البلدان الأخرى.
- إنشاء شبكات استشعار الداتا الحكومية من أجل تحصيل معلومات في الوقت الحقيقي والمناسب حول قطاعات الأمن والنقل والصحة والمناخ والبيئة وغيرها. مع ما يعني ذلك من تخصيص قدرة حاسوبية ومركز داتا خاصة بإستقبال ومعالجة وتخزين داتا الاستشعار تلك.
- الاستثمار في وسائل الدفع الالكتروني عبر الهواتف الذكية من أجل تمكين المواطن من تسديد رسوم الخدمات مباشرة عبر المحفظة الرقمية التي يحملها في هاتفه الذكي (من قبيل دفع رسوم حافلات النقل والمترو والمواقف العامة وغيرها عبر هاتفه الجوال).
- الانتقال تدريجياً إلى نموذج السحابة الالكترونية (Cloud Computing) من أجل تأمين القدرة الحاسوبية ومخازن الداتا على الطلب لمختلف الأجهزة الحكومية والوزارات. وهذا النموذج بدأ يثبت نجاحه في مختلف قطاعات الأعمال حيث تمكنت الكثير من المؤسسات من

حيازة قدرة حاسوبية هائلة (مئات السيرفيرات) من أجـــل إجراء عملية تحليل عميقة على الـــداتا المختلفـــة ثم تقـــوم بالتخلص من تلك السيرفيرات بعد إنتهاء المطلـــوب منـــها حيث يجري العمل على تدويرها وإعادة تأجيرها ثانية.

وكما أن أي تحوّل تقني جذري لا بد من أن يتم مجاراته بتطـــوير تنظيمي وإداري وتشريعي، من المهم أن تعمد الحكومـــة المركزيـــة إلى العبور نحو الحكومة الذكية عبر سلســـلة مـــن الإجـــراءات الاداريـــة والتنظيمية والتي سوف تضمن إدارة مشاريع فعّالة وإلتزام قوي بـــأمن معلومات الأفراد والمؤسسات وكذلك التأكد من تطـــوير القـــدرات البشرية التي تملكها من أجل مجاراة النقلة الذكية. إن الحكومة الذكيـــة بحاجة إلى مجتمع ذكي والمجتمع الذكي بحاجة إلى أفراد أذكياء والأفراد الأذكياء بحاجة إلى تعليم ذكي وتستمر السلسلة، ولذلك فإن تطبيـــق الحكومة الذكية في أحد البلدان سوف يعتبر مؤشراً قوياً على مســـتوى تقدم شعوب ومجتمعات تلك البلدان.



رسم توضيحي 1: الإطار المرجعي للحكومة الذكية

إن الحكومة الذكية هي حكومة جوّالة (Mobile Government) تنشر خدماتها بكفاءة على الأجهزة الذكية المحمولة، وهـي حكومـة حسّاسة (Data Sensing Government) تلتقط ما ينتشر حولها مـن داتا وتستفيد منها، وهي حكومة مطّاطـة (Elastic Government) تستوعب الطلب المتزايد على الطاقة الحاسوبية بكفاءة وهي حكومـة إجتماعية (Social Government) تتواصل مع جمهورها ومواطنيهـا بشفافية وإنفتاح وعبر مختلف الشبكات الإجتماعية الالكترونية المتوفرة.

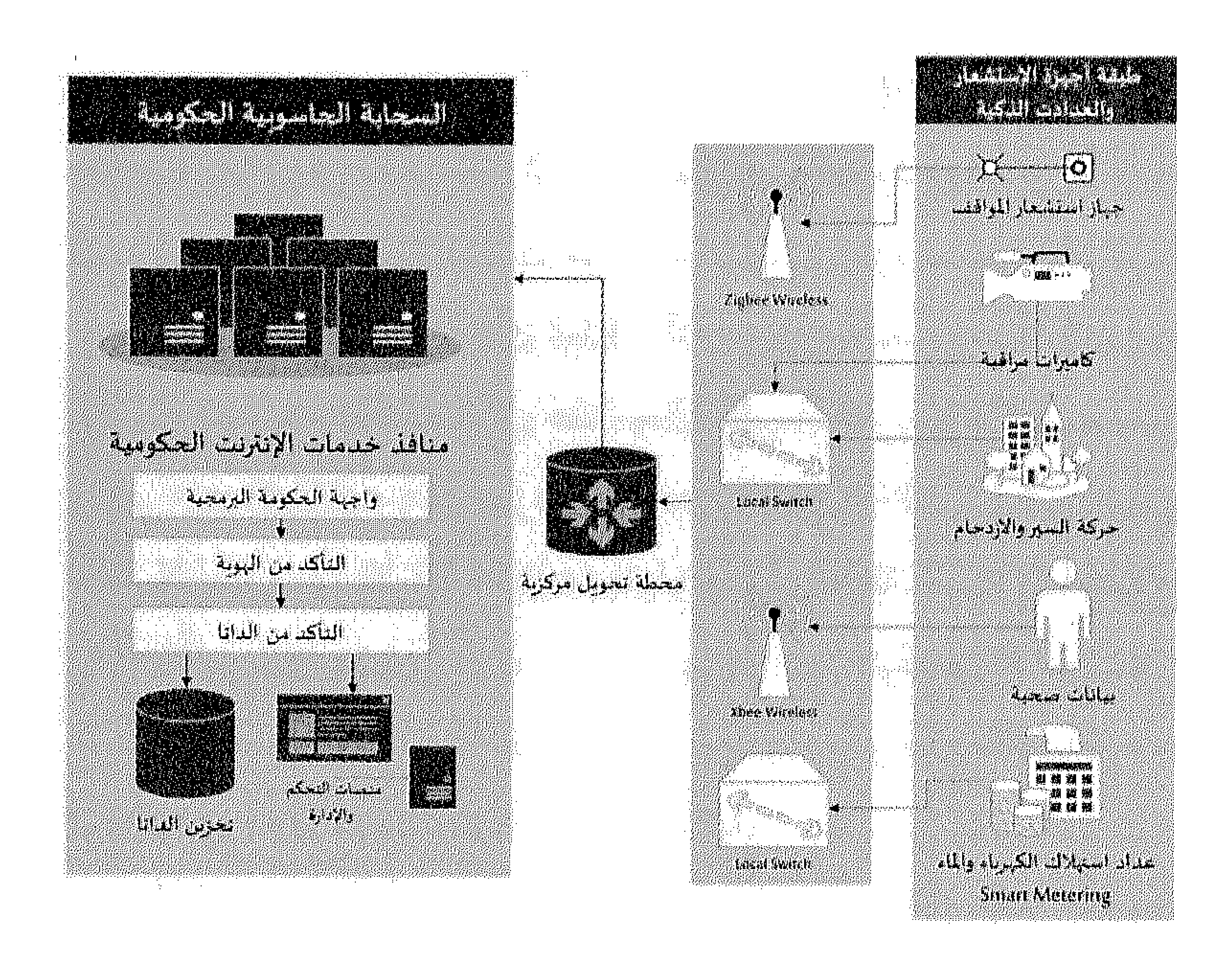
شبكة أجهزة الاستشعار الذكية

تطورت أنظمة التشغيل الصغرية (Micro Operating System) وإمكانية تضمينها في أجهزة الاستشعار المختلفة مع قدرتها على الوصول إلى الشبكات الخاصة وشبكات الإنترنت عبر مجموعة بروتوكولات نقل الداتا بين جهاز الاستشعار وخوادم المؤسسة أو الحكومة، وقد قامت العديد من الدول والحكومات حول العالم بإنشاء شبكات الأشياء (Internet of Things) والتي تقوم بتجميع الداتا المختلفة بطريقة أوتوماتيكية من مصادر معلومات قطاعية ونذكر منها:

- **الداتا الأمنية:** والتي يتم تجمعيها من شبكات كاميرات المراقبة والتي تعمل من خلال بروتوكول الإنترنت. حيث يتم تخزين هذه الداتا وصيانتها وتحليلها من أجل كشف الجرائم أو البحث عن تقاطعات أمنية حدثت في بعض الأماكن وغيرها من الأمور التي تهم أمن الدولة.
- **الداتا المناخية:** وقد أصبح بإمكان الحكومة معالجة داتا المناخ مباشرة داخل مراكز الداتا الخاصة بها بعد إن تمكنت[1] من زرع أجهزة إستشعار مناخية مرتبطة بسحابة الحكومة الالكترونية وموزعة على مختلف المناطق الجغرافية في الدولة.
- **الداتا الصحية من الأفراد:** وقد تشكل هذه التقنية ثورة في عالم متابعة الأفراد المرضى والذين لا يجدون من يراقبهم

طوال الوقت. وسوف تسمح أجهزة الإستشعار الشخصية بقياس مستويات السكر والضغط من مريض معين على سبيل المثال وإرسال تلك المعلومات بطريقة دورية إلى الأطباء المعالجين مع إمكانية إرسال إنذارات عبر جوال أولئك الأطباء إذا تجاوزت تلك الداتا المعدلات الصحية المسموح بها.

- **الداتا المنزلية:** وهو نفس مفهوم المنزل الذكي حيث ترتبط أجهزة الإستشعار المنزلية بشبكات الإنترنت من أجل إدارة أنظمة المنزل عن بعد والتحكم بها ومعرفة ما يحصل داخل المنزل خلال الابتعاد عنه. وسوف يصبح المواطن قادراً مباشرة عبر جهازه الجوال على معرفة ما إذا تجاوز مصروفه للخدمات الكهربائية أو المائية حداً معيناً أو إذا ما قام أحدهم بإقتحام منزله أو حتى تشغيل وإيقاف أجهزة التبريد والتسخين عن بعد على سبيل المثال.
- **الداتا الحكومية الخدمية:** هل سوف نقول وداعاً لجابي فواتير الكهرباء؟ ربما فقد أصبحت ساعة الكهرباء جهازاً ذكياً يقرأ مصروف المنزل أو المؤسسة ويقوم بإرسال تلك المعلومات إلى خوادم شركات الكهرباء بطريقة مباشرة حيث يتم إحتساب الفواتير وإدخالها إلى الأنظمة المالية الحكومية بطريقة أوتوماتيكية، وينسحب هذا الأمر على مختلف الخدمات الحكومية التي تحتاج إلى قياس المصروف والاستهلاك مثل المياه والنفط والغاز وغيرها.



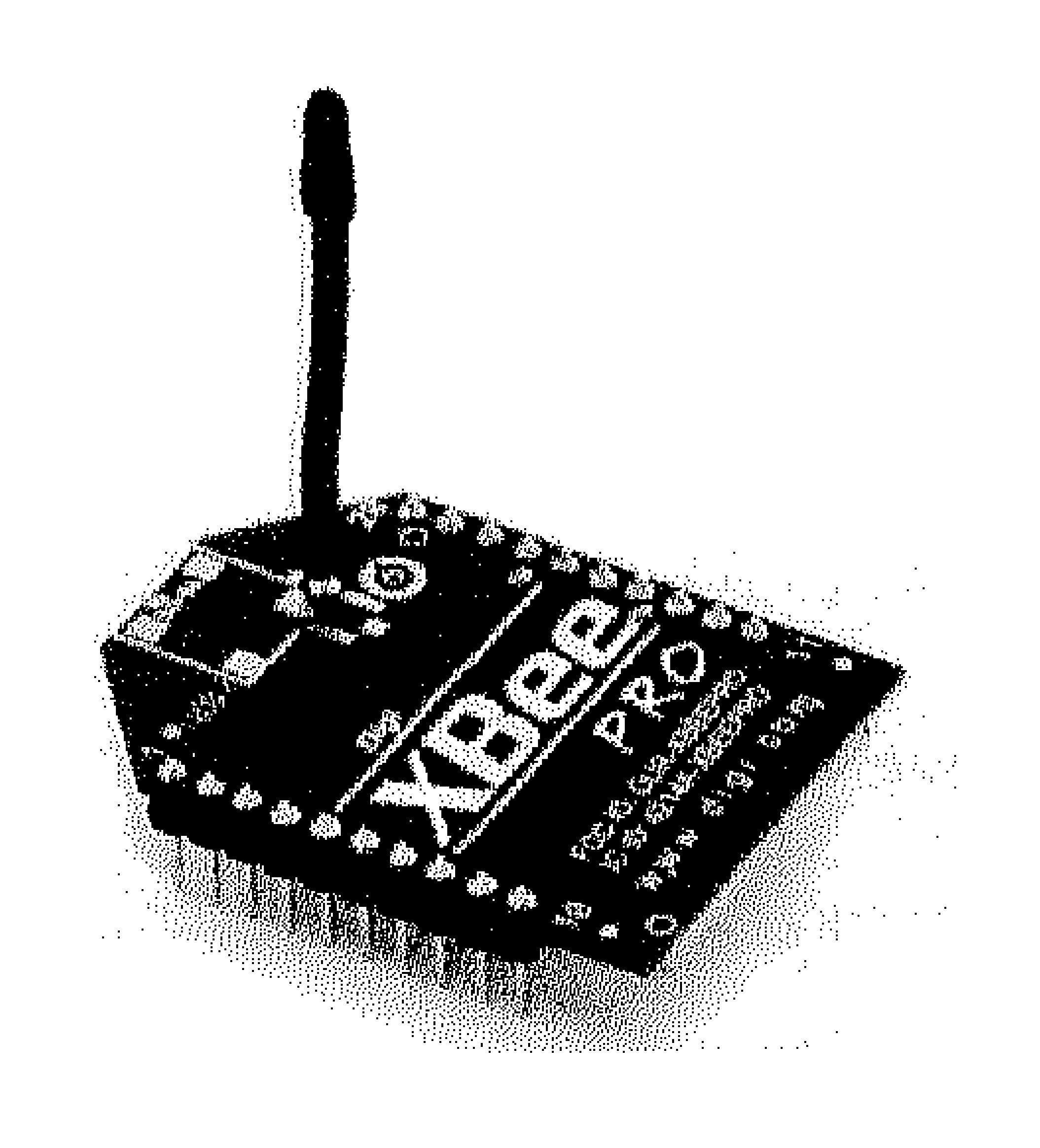
رسم توضيحي 2: شبكة أجهزة الاستشعار وعدادات الخدمات الذكية

ومن أجل الإستفادة القصوى تقوم الحكومة ببناء سحابة حاسوبية خاصة بإستقبال داتا أجهزة الإستشعار من مختلف النقاط والأشياء الذكية المنتشرة في القطاعات المجتمعية المختلفة مثل الصحة والنفط والتخطيط المدني والماء والكهرباء وباقي القطاعات التي ينتج عنها داتا تحتاج إلى التحليل والحفظ والمحاسبة والمراقبة.

بروتوكولات الوايرلس الخفيفة

تحتاج حكومة الأشياء (Government of Things) إلى وسائط من أجل نقل الداتا من أجهزة الإستشعار والأدوات الإلكترونية الأخرى إلى شبكة الحكومة وفي كثير من الأحيان لا يكون الربط السلكي عملياً او متاحاً لتلك "الأشياء الذكية" من أجل توصيلها

بالشبكة، وقد ظهرت بروتوكولات الواي فاي (WiFi) والبلوتـــوث (Blootooth) من أجل نقل الداتا بطريقة لاسلكية ولكن تعاني الأنظمة التي تعتمد تلك البروتوكولات من حاجتـــها إلى تزويـــدها بالطاقـــة بإستمرار حيث تستهلك تلك الطاقة لأن معدل وحجم إرسالها للـــداتا عالي. وقد عمل المطوّرون في هذا المجال على إبتكار بروتوكول قياسي يسمى (ZigBee) ويتميز بترداد منخفض للداتا في الثانية يكفي مـــن جهة لإرسال داتا الأجهزة الإستشعار ويقتصد الطاقة حيث لا تحتـــاج تلك الأجهزة إلى شحن او تغيير بطاريتها إلا بعد فترة طويلة تتجـــاوز السنة في بعض الأحيان مما يجعلها عملية وإقتصادية وخفيفة الصيانة عند تركيبها في أجهزة إستشعار الحكومة الذكية.



رسم توضيحي 3: شريحة وايرلس اكس بي برو

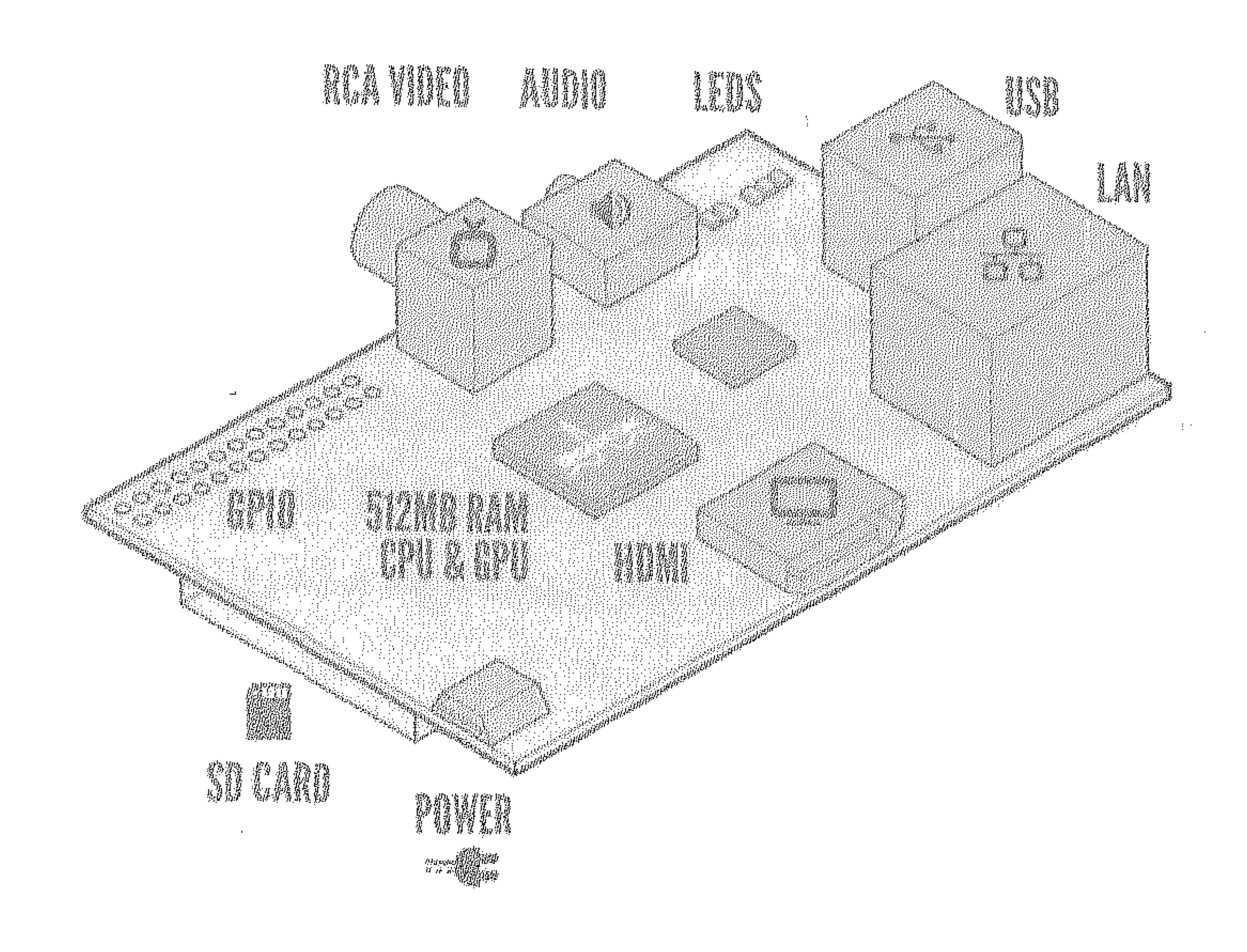
وتوضح لنـــا الصـــورة إعـــلاه شـــريحة وايـــرلس مـــن طـــراز (XBee PRO) والتي يمكن أن يبلغ مداها إلى ما يقارب واحد كيلـــومتر ونصف ويمكن شبكها بجهاز اردوينو أو راسبري باي من أجـــل إرســـال الداتا المستخرجة من قطاع البيئة او قطاع الأمن وغيرهما مباشرة إلى محول داتا مركزي (Local Switch) مرتبط بالسحابة الحاسوبية الحكومية.

الأجهزة الحاسوبية المضمّنة

مع إزدياد الحاجة إلى إلتقاط الداتا من مختلف القطاعات الإجتماعية والإقتصادية والحكومية سوف يزداد الطلب على الطاقة الحاسوبية الموضعية (Local Computing) وهذا يعني أن جهاز الإستشعار الذكي، على سبيل المثال، قد يتم ربطه بمعالج ضمني يقوم بإجراء العمليات الحاسوبية الموضعية على الداتا المستخرجة من ذلك الجهاز قبل إرسالها إلى شبكات الحكومة أو قد تكون مهمة المعالجات الحاسوبية تلك محلية مثل الأجهزة التي تعمل على تنظيم إنارة الطرقات بطريقة ذكية.

وقد ظهر نموذجان ناجحان لتلك الأجهزة الحاسوبية وهما (Arduino) و(Raspberry PI) حيث يحتوي الأول على معالج صغير وذاكرة عشوائية الوصول ومنفذ بيانات خارج-داخل بينما يعتبر الثاني جهاز كمبيوتر متكامل صغير من دون الطرفيات. وبالإمكان تضمين الكثير من التطبيقات الحكومية في تلك الأجهزة الصغرية والتي تتميز بقلة إستهلاكها للطاقة وامكانية تركيبها في الكثير من الأمكنة العامة والخاصة والآلات ومنها مركبات النقل العام ومحطات الإنتظار والمرافق الحكومية العامة وتنظيم عملية الإنتظار في صفوف الخدمة وغيرها من التطبيقات مثل تجهيز تلك الأنظمة بكاميرات مراقبة وتسجيل الحركة والصوت في الأماكن الأمنية المهمة وتوظيفها في عملية التحكم عن بعد.

وتعتبر إضافة هذه "العقول الإصطناعية" الصغيرة إلى طبقات الحكومة الذكية من الإضافات المهمة التي سوف تدفع بعملية الإبتكار والإبداع في الدولة وتشجع القطاع العام والخاص على تطوير تطبيقات خدمية تعتمد على الميزات التقنية التي تتمتع بها تلك الأجهزة.



رسم توضيحي 4: مكونات جهاز راسبري باي

وتمثل هذه الأجهزة وأنظمة تشغيلها مجالاً خصباً للإستثمار في القطاع التعليمي والأكاديمي حيث يمكن للحكومة أن تزود بها مختبرات المدارس من أجل تشجيع الطلاب على بناء تطبيقات ذكية عليها والإستفادة من المشاريع الناجحة لاحقاً عبر تبنيها والإستثمار فيها وصولاً إلى وضعها في الخدمة الفعلية للحكومة.

وكما في أي تقنية تدخلها الحكومة إلى جسمها الإداري والتنظيمي يجب أن تخضع تلك الأجهزة والتطبيقات إلى معايير خاصة بأمن المعلومات وأمن الأجهزة المادي وكيفية تواصلها مع أنظمة الحكومة المختلفة والتأكد من عدم سرقتها أو سرقة منافذها الإلكترونية وتسميم الداتا الحكومية بداتا تضليلية.

لقد قدمنا نموذجاً عن ما يمكن ان تؤول إليه شبكات الحكومة الذكية في المستقبل القريب، وأمثلة التطبيقات الاستشعارية كثيرة جداً في مجال تدعيم العمل الحكومي وإراحة المواطن من عناء متابعة خدماته وتركه يقوم بالتركيز على ما هو أهم بالنسبة له.

سوف يؤدي هذا التطور في الالكترونيات الاستشعارية وقدرتها على الارتباط بالشبكات ومنها شبكة الإنترنت إلى ولادة "حكومة الأشياء Government of Things" قريباً جداً.

الداتا الحكومية الضخمة

"تحليل الداتا الضخمة يؤدي إلى التنبؤ بسلوكيات الأفـراد في العالم الافتراضي"

الدكتور اريك سيغل

بما أن الحكومة هي اللاعب الأكبر في المجتمع ونظـراً لتشـعب علاقاتها مع المواطنين ومؤسسات الأعمـال والحكومـات الأخـرى فسوف ينتج عن ذلك حركة بيانات وداتا ضخمة جداً عادةً ما تكون موزعة على الأجهزة العامة والإدارات الرسمية والوزارات ومراكز أخذ القرار في الدولة، ولطالما كانت الحكومة بشكل عام حساسة تجاه فتح الداتا أمام الجمهور ولكن التطورات السياسية الحديثـة والإنفتـاح الاقتصادي العالمي الذي تشهده الدول وضرورة تعاونها مع بعضـها البعض فرض على تلك الحكومات أن تنتهج نهجاً أكثـر مرونـة في التعاطي مع المعلومات الحكومية العامـة ولم يعـد بإمكـان تلـك الحكومات أن تكون شفافة من دون كشف المزيد من البيانات (على كل حال البيانات التي يطالب بكشفها الجمهور هي عـادةً بيانـات مالية وإقتصادية وتجارية من أجل مراقبة الحكومة ومحاربـة الفسـاد وبالتالي فإن المعلومات العسكرية والأمنية التي تخص أمن الدولة هـي خارج الموضوع بشكل عام).

وقد تحتاج عملية توفير الداتا الحكومية الضخمة على الإنترنت بشكلها الخام إلى بعض التشريعات والقوانين بالاضافة إلى العمل الفني والتقني الذي سوف يقوم به فريق الداتا الحكومية من تخزين وصيانة وبرمجة منافذ الوصول إلى تلك الداتا عبر شبكة الإنترنت.

مركز الداتا الحكومية

نظراً لأهمية الداتا الحكومية وتأثيرها على الرأي العام والاقتصاد المحلي وتطور الأعمال وخلق فرص عمل جديدة، فقد تعمد بعض الحكومات إلى إنشاء مركز موحّد للداتا الحكومية يكون من مهامه تجميع الداتا المفتوحة وفقاً للقوانين والتشريعات المعمول بها في الدولة ونقلها بطريقة دورية إلى مخازن الداتا الحكومية الخاصة بمركز الداتا ثم التأكد من تنظيفها من الشوائب وجعلها متوفرة على خوادم الوب بصيغة خام لطيفة واهمها النسق JSON وتوفير واجهة تطبيقية قياسية حيث يتمكن المبرمجون المستقلون أو الشركات من تطوير تطبيقات جوالة وتطبيقات إنترنت بالاعتماد على تلك الداتا. وهكذا تكون الحكومة وفي نفس الوقت الذي مارست فيه المزيد من الشفافية، تكون قد قامت بتأمين مجالات إبتكار وفرص عمل لخبراء المعلوماتية في البلد والأهم من ذلك أن المواطن سوف يستفيد من تنوع التطبيقات والمنافسة فيما بينها من أجل تقديم الخدمة الأفضل.

مخزن التطبيقات المستفيدة من الداتا الحكومية

قد يسيء البعض إستخدام الداتا الحكومية عن قصد أو عن غير قصد وربما يؤدي هذا الأمر إلى الاساءة إلى المواطنين عبر تحصيل معلومات خاصة منهم بطريقة غير مشروعة أو ربما يتم "تسميم" الداتا

من قبل جهات غير معروفة عبر بناء تطبيقات حكومية مزيفة من أجل نشر فيروسات التجسس وغيرها من البرامج الخبيثة والملوثة على أجهزة المواطنين ولذلك من المهم أن تقوم الحكومة بفرض إجـــراءات رقابيـــة على التطبيقات التي سوف تستفيد من الداتا الحكومية الضخمة ومـــن تلك الإجراءات:

- إعتماد مخزن تطبيقات موحد يتم من خلاله نشر تطبيقـــات الجمهور المستفيد من الداتا الحكومية المفتوحة والتي تمـــت الموافقة عليها من قبل إدارة الحكومة الذكية.
- إعتماد مفاتيح الاتصال بواجهـــة الـــداتا الحكوميـــة مـــن أجل حصر المتصلين ومعرفـــة حركـــة اتصـــالهم بالـــداتا (Gov Data API – ACCESS KEY) وتحديد حجـــم اتصالاتهم اليومية من أجل عدم إغراق الشبكات الحكومية.
- ضرورة التقدم بطلب صغير من قبل المبرمجين يوضح للجهة الحكومية ماهية التطبيق وكيفية استخدامه وأي نوع مـــن الداتا الحكومية مطلوبة.
- إخضاع تلك التطبيقات الحكومية لعدد من الفحوص التقنية في المختبر الرقمي للتأكد من خلوها من الـــبرامج الملوثـــة ومعرفة مسار الداتا الصادر منها وإليها.

وتماماً كما يوجد الكثير من مستودعات التطبيقات (مثل غوغـــل بلايستور وأبل ابستور) يمكن إنشاء مستودع التطبيقـــات الحكوميـــة (Gov App Store) والذي يتحوي على التطبيقات التي يقوم بتطويرها العامة والجمهور والشركات والمبرمجين المستقلين والتطبيقات الحكومية الرسمية.

نحو فدرالية الداتا الحكومية؟

ونعني بالفدرالية هنا مركزية الداتا من حيث منافذ الخدمة وليس بالضرورة مركزيتها من حيث الإنتاج وذلك لتعقد حركة نقل الداتا الحكومية المختلفة من الدوائر الرسمية والوزارات كافة إلى مركز واحد يقع على عاتقه عملية استقبال الخدمات الزراعية والاقتصادية والسياحية وغيرها على سبيل المثال وينتج عن معاملاته كافة أنواع الداتا. وتطرح عملية تخديم الداتا الحكومية من منفذ مشترك على الإنترنت أو السحابة الحاسوبية الحكومية عدة تحديات وتساؤلات ينبغي الإجابة عليها حسب طبيعة كل حكومة وليس بالضروري ما يكون مفيداً وفعّالاً لحكومة ما أن يكون بنفس المستوى من الفعالية لحكومة اخرى. وعلى كل الأحوال يتم "فدرلة" الداتا الحكومية عبر واحدة من طريقتين:

1. نقل الداتا دورياً كلما تجمعت من الدوائر الحكومية والوزارات وجعلها متوفرة في المركز الرئيسي للداتا الحكومية حيث يتم التأكد من مطابقتها للمعايير وتنظيفها من الشوائب وتخديمها بالطريقة القياسية التي تفرضها إدارة الحكومة الذكية. ويمكن أن يكون النقل أوتوماتيكياً عبر بناء مجموعة من نواقل الداتا (Gov Data Bus) تعمل وفقاً لبرمجة زمنية معينة وتقوم بنسخ الداتا الجديدة المتوفرة في أجهزة الدولة المختلفة إلى أجهزة مركز الداتا الحكومية المركزية ويمكن استخدام بروتوكولات نقل الداتا المعروفة (FTP, SCP, HTTP, etc...).
2. بناء بوابة إنترنت مركزية في مركز الداتا الحكومي ونشر كتالوغ الداتا الحكومية (Gov Big Data Catalogue) المتوفرة في مختلف الوزارات والإدارات العامة مع طريقة

النفاذ إليها ونسق الداتا المتوفر وغيرها من المعلومات الـتي تساعد مبرمجو القطاع الخاص والمستقلون على بناء تطبيقات حول تلك الداتا.

وبالتأكيد فإن لكل نموذج إيجابياته وسلبياته ويلخص الجدول التالي بعض مميزات كل نموذج وبعض العوامل التي يجب أخذها بعين الإعتبار عند تصميم الداتا الحكومية الضخمة:

	النموذج المركزي للداتا الحكومية	النموذج اللامركزي للداتا الحكومية
الالتزام بالمعايير القياسية	يتم التأكد من الالتزام بالمعايير القياسية مركزياً وعبر فريق عمل متخصص وغالباً ما تكون المعايير محترمة أكثر في هذا النموذج.	تنشر الحكومة مجموعة المعايير للداتا الحكومية الضخمة وتترك الالتزام بها للوزارات المختلفة والتي قد لا تلتزم بها كلياً.
أمن الداتا الحكومية	أمن مركزي غير مشتت وفي أغلب الأحيان يكون قوي	أمن مشتت غير مركزي ومن الممكن أن يكون عرضة للإختراق
سرعة توفر الداتا	تعتمد سرعة وفرة الداتا على عملية النقل والتنظيف والتحضير للخدمة وعادة ما تكون أبطأ من النظام اللامركزي	الداتا الحكومية تصبح متوفرة مباشرة بعد الإنتاج
مستوى توفر الخدمة	تعتمد خدمة الداتا هنا على أنظمة وأجهزة مركز الداتا الحكومي واذا حصل خلل فيه فإن كل الداتا تصبح غير متوفرة دفعةً واحدة	تتوفر الخدمة في أنظمة الوزارات المختلفة ولا يؤثر توقف أنظمة وزارة معينة عن العمل على توفر الخدمة في وزارات أخرى.

جدول 2: مركزية الداتا الحكومية الضخمة

وينبغي الإشارة إلى أن لدى الداتا الضخمة خاصيتان اساسـياتان تميزها عن الداتا التقليدية التي تعاملنا معها لسـنوات طويلـة وهمـا: الإختلاف في طريقة تمثيل الداتا عبر الانتقال من نموذج الجداول والداتا العلائقية إلى الداتا الشبكية (Graph and Document Based Data) والميزة الثانية هي حجم تلك الداتا حيث نتعامل في الداتا الضخمة مـع متطلبات تخزين كبيرة لا تكفيها وسائط التخزين العادية بل تحتـاج إلى مصفوفة وسائط تخزين مرتبطة مع بعضها البعض ويتم إدارتها عبر انظمة حديثة مثل Hadoop File System.

الحوسبة السحابية في الحكومة

"السحابة الحاسوبية هي طريقة جديدة لبناء التطبيقات وليس فقط مكان تواجد هذه التطبيقات"

بول ماريتز

في البداية كانت مراكز الداتا

من اجل فهم طبيعة وفوائد الحوسبة السحابية لا بد من العودة إلى الخلف قليلاً لنرى كيف كانت المؤسسات والحكومات تحصل على القدرة الحاسوبية وأماكن تخزين الداتا، فنحن نعلم أن معظم تلك الكيانات والتي كانت تعتبر متقدمة في هذا المجال كانت تعتمد على بناء مراكز داتا خاصة بها (Data Centers) من أجل فدرلة الحوسبة (Centralized Server Side Computing) والتخزين، وتلك الكيانات الأقل تطوراً كانت ولا تزال تتعامل مع طاقة حاسوبية مبعثرة وموزعة على الأقسام داخلها (In-department Servers)، ويعتمد مبدأ بناء مركز داتا موحّد على تجميع الخوادم الأساسية وأنظمة الحماية والبنية التحتية الشبكية للمؤسسة في مكان واحد وتهيئة ذلك المكان من ناحية التبريد والتكييف وأنظمة الطاقة الكهربائية الاصيلة والرديفة وحماية ذلك المكان بأنظمة وإجراءات الدخول وتزويده بوصلات إنترنت عالية السعة. وعادة ما يحتوي مركز الداتا الحكومي أو

المؤسساتي على الأنظمة الخاصة ببوابات الإنترنت وأنظمة إدارة الأعمال الرئيسية مثل شؤون الموظفين والمحاسبة والتسويق وإدارة الوثائق والمحتوى وأنظمة البريد الالكتروني وغيرها بينما تقتصر محطات الحوسبة لدى الأفراد في مختلف الأقسام على البرامج المكتبية ومتصفحات الإنترنت والبرامج التي يستعين بها الموظف من أجل أداء أعماله اليومية.

وقد ساعدت مراكز الداتا الحديثة داخل المؤسسات على تقديم حماية أفضل للمعلومات والبيانات المركزية بالاضافة إلى دورها الرئيسي في تقديم قدرة حاسوبية مركزية تستفيد منها كافة الأقسام من دون عناء الاهتمام بالسيرفيرات وصيانتها وتحديث برامجها حيث تقع تلك المسؤوليات على عاتق فريق إدارة مركز الداتا.

ولكن هذا النموذج وبالرغم من كل حسناته كان يعاني من عدة نقاط ضعف وأهمها:

ضعف المرونة في التوسّع والإنكماش

تصور لو ان حكومة معينة كانت بحاجة إلى إجراء عمليات حاسوبية معقّدة مثل عمليات إيجاد الأنماط (Pattern Recognition) في التحليل الطبي او البحث الجنائي الأمني أو حتى عمليات معالجة كمية كبيرة من الصور والوسائط والفيديو حيث يتطلب كل ذلك قدرة حاسوبية كبيرة وسعة تخزين واسعة فسوف تكون الحكومة مضطرة إلى شراء المزيد من السيرفيرات وتجهيزها وربطها بشبكة مركز الداتا ثم تحميل البرامج عليها من أجل إجراء تلك العمليات المذكورة وتسمى هذه المرحلة "مرحلة التوسّع الحاسوبي" حيث تكون في أغلب الأحيان مكلفة مادياً وبشرياً وتستنزف طاقات المؤسسة أو الحكومة. وبعد إجراء كل تلك العمليات الحاسوبية قد تقرر الحكومة

أن تلك السيرفيرات الجديدة تستهلك الطاقة والصيانة ولا يتم إستخدامها كلياً ويمكن بالتالي الإستغناء عنها وتسمى هذه المرحلة "مرحلة الإنكماش الحاسوبي" وهي سوف تكون مكلفة أيضاً لأن إحالة تلك السيرفيرات وأنظمة التخزين على التقاعد أو وضعها من دون عمل يعني أنها تفقد قيمتها عبر الزمن وسوف تصبح دون قيمة بعد فترة نظراً لسرعة تطور العتاد الحاسوبي.

تشتت إدارة المعلومات عن المهمة الرئيسية للحكومة

إن إدارة مركز الداتا سوف تأخذ تأخذ حيزاً مهماً من الوقت الثمين لإدارة المعلوماتية سواء في المؤسسة او الحكومة وبدلاً من التركيز كلياً على تطوير الأنظمة التي تخدم المواطنين بطريقة سليمة وفعّالة ودراسة ملاحظات أولئك المستخدمين والعمل على التحسين المستمر، سوف يتم استهلاك الوقت الاداري والبشري في ملاحقة انظمة الطاقة في مركز الداتا والتأكد من أن أنظمة التكييف والتبريد شغالة على مدار الساعة حتى لا تصاب الأجهزة بالخلل من جرّاء الحرارة الناجمة عن تشغيل الأجهزة والتأكد من سلامة إجراءات الأمن المادية المتعلقة بالمكان والعمل بشكل دوري على إستبدال وسائط التخزين حتى لا تصاب بالتلف والكثير من الأمور التي يجب على إدارة المعلوماتية أن تعالجها في مركز الداتا.

تعقيدات إدخال أنظمة جديدة

قد تحتاج إدارة المؤسسة إلى إدخال نظام جديد مثل وسيط الأنظمة (Middleware) إلى منظومتها وذلك من أجل دعم نظام مركزي أو نظامين ويعني إدخال مثل هذا النظام أن على المؤسسة أن

تستحوذ على المهارات البشرية المتخصصة بتركيب وتهيئة النظام الوسيط وتشغيله والتأكد من توافريته على مدار الساعة (Availability) وكل ذلك يجب أن يتم حتى قبل أن يبدأ المبرمجون بالعمل عليه والاستفادة منه وناهيك عن السيرفيرات المطلوب شراؤها والقدرة على التمدد العامودي أو الأفقي على الطلب.

كل ما تقدم دفع بالمؤسسات والحكومات إلى المطالبة بحلول جديدة أكثر مرونة وأقل كلفة على المدى الطويل وكذلك أقل تطلباً للمهارات البشرية والاهم من ذلك كله هي الحلول التي تسمح لتلك الكيانات بالتركيز أكثر على مهمتها الرئيسية التي وُجدت من أجلها. ما رأيكم بالطاقة الحاسوبية على الطلب؟ وإمكانيات التخزين اللامتناهية السعة؟ مرحباً بالحوسبة السحابية!.

ما هي الحوسبة السحابية؟

ظهر مفهوم الحوسبة السحابية في العقد الماضي وقد تطور بشكل كبير خاصة بعد أن أثبتت أنظمة التشغيل الافتراضية (Virtualization) فعاليتها في تقسيم موارد الآلة المادية من معالجات وذاكرة وصول عشوائي إلى شبه خوادم تعمل بصورة مستقلة عن بعضها البعض وأصبح بالإمكان تشغيل العديد من أنظمة التشغيل على نفس الأجهزة والسيرفيرات بحيث تتقاسم موارد تلك الأجهزة وتظهر للمستخدم على أنها سيرفيرات مستقلة (Virtual Private Servers) وقد قامت كبرى الشركات العالمية وعلى رأسها شركة أمازون وراكسبايس وآي بي آم ومايكروسوفت (Amazon, Rackspace, IBM & Microsoft) بأخذ هذا النموذج إلى المستوى التالي من التطور حيث عمدت إلى إنتاج برمجيات قادرة على مكننة عملية إضافة السيرفيرات الافتراضية وفوترة وقت إستخدامها وإعادة

تدويرها من أجل الاستفادة من الموارد الحاسوبية مجدداً. وقد أدى تطــور الحوسبة السحابية والمنافسة بين تلك الشركات إلى إنتـــاج مراكـــز داتـــا إفتراضية ضخمة جداً يمكن للزبائن ان يستأجروا فيها العدد الذي يريدونـــه من سيرفيرات الحوسبة مع إمكانية تحديد الموارد المطلوبة من قبيل الـــذاكرة العشوائية ومخازن الداتا وعدد المعالجات وكل ذلك يتم إجراؤه أوتومياتيكياً من خلال مواقع الإنترنت المخصصة لذلك أو حتى عبر استخدام واجهات البرمجة التطبيقية (Cloud API) لمكننة تلك العملية مـــن داخـــل بـــرامج الحكومة أو المؤسسة مباشرة.

ميزات الحوسبة السحابية	
الطاقة الحاسوبية المطاطة (Elasticity)	إمكانية الاستحواذ على موارد وطاقة حاسوبية بسهولة مع القدرة على التخلص منها بسهولة أيضاً.
تدوير الموارد الحاسوبية (Recycling)	إعادة إستخدام الموارد الحاسوبية مباشرة بعد تحريرها من زبون سابق.
إدفع بقدر الاستخدام (Utility Service Model)	اذا استخدمت تخزين بسعة 100 جيجابايت مثلاً فأنت تدفع فقط لهذه السعة وليس أكثر وكذلك الأمر بالنسبة لوقت المعالجة وتدفق الداتا عبر الشبكة.
أخدم نفسك بنفسك (Self-Service)	يستطيع الزبون مباشرة وعبر واجهة التحكم من خلال المتصفح أن يزيد عدد سيرفيراته أو يقوم بتحرير وحذف بعضها أو إضافة قواعد بيانات في الكلاود وصولاً إلى إجراء كافة العمليات الادارية مباشرة من دون الحاجة للرجوع إلى الشركة عن عمليات الاستحواذ على الطاقة الحاسوبية

جدول 3: ميزات الحوسبة السحابية

ومن هنا أصبح نموذج الحوسبة ومواردها بشكل عام يشبه إلى حد كبير نموذج الخدمات الكهربائية والمائية حيث يشترك الزبون بحساب في شركة الحوسبة السحابية ويدفع تلقاء إستخدامه للموارد والسيرفيرات والتخزين وحين لا تكون تلك الموارد مستخدمة فإنه ببساطة لا يدفع تماماً مثل فواتير الكهرباء والماء حيث يدفع المشترك مقابل استهلاكه وبالتالي تستطيع الحكومة او المؤسسة الاستحواذ على طاقة حاسوبية كبيرة تستخدمها لمدة معينة مثل معالجة كم كبير من الصور أو تحليل داتا معقّدة ثم تستغني عن تلك الطاقة ببساطة من دون أن تكون قد قامت بشراء أية أجهزة أو تكبدت عناء تحميل أنظمة التشغيل وإلى ما هنالك من متطلبات إدارية لكل تلك العملية.

نماذج الحوسبة السحابية

يوجد عدة نماذج لتقديم الخدمة الحاسوبية على الطلب وقد تم تشخيص ثلاثة نماذج على المستوى العالمي وهي:

Government as a Service

IaaS PaaS SaaS

تطبيقات الأعمال

الأنظمة الوسيطة والخدمية

مسؤولية الحكومة

مسؤولية مزود الخدمات

رسم توضيحي 5: الحكومة كنموذج خدماتي سحابي

البنية التحية على الطلب (IaaS)

بشكل عام في هذا النموذج يتم تقديم السيرفيرات على الطلب وكذلك عملية الاتصال بالإنترنت والشبكة الداخلية وعناوين الآي بي الخاصة (Private IPs) ووسائط تخزين الداتا ويمكن للزبون إختيار عدد المعالجات (Processors) وحجم الذاكرة العشوائية الوصول وحجم التخزين في كل سيرفير يقوم بإستئجاره ومثال على ذلك الخوادم على الطلب من شركة امازون EC2 servers والتي يمكن الاستحواذ عليها بطريقة سهلة جداً وإختيار أنظمة التشغيل فيها (ويندوز أو لينكس) وبعدها يستطيع الزبون الحكومي أو المؤسسي أن يتعامل مع تلك السيرفيرات عن بعد من أجل تركيب مختلف البرمجيات فيها. ويطلق على هذا النموذج إسم Infrastructure as a Service.

ومن الممكن الذهاب بعيداً في هذا النموذج إلى حد إنشاء مركز داتا متكامل إفتراضي يحتوي على العديد من الخوادم مرتبطة شبكياً مع بعضها البعض ومحمية امنياً بحيث لا يمكن الدخل إلى تلك الأجهزة إلى عبر شبكة خاصة (Virtual Private Network). وعادةً ما تقوم الحكومات المتقدمة بإنشاء مراكز داتا إفتراضية (Virtual Private Cloud) وتربطها بمراكز الداتا الخاصة بها عبر وصلات إنترنت مخصصة حيث تستخدم تلك الطاقة الحاسوبية الممتدة من أجل تأمين التوافرية على الإنترنت وأخذ النسخ الإحتياطية وإجراء عمليات المعالجة المعقّدة.

الأنظمة الوسيطة على الطلب (PaaS)

وهنا يأخذ مزودو خدمات الكلاود النوذج السابق إلى المستوى التالي وبدلاً من الاقتصار فقط على تأمين الخوادم المجهزة بأنظمة تشغيل فقط، تقوم تلك الشركات بتركيب أنظمة وسيطة وخدمية مثل نظام

التراسل بين الأنظمـــة (Middleware) وأنظمـــة قواعـــد البيانـــات (Databases) وحاويـــات الـــبرامج (Web containers) وأنظمـــة الدخول والتأكد من الهوية (Authentication providers) وغيرها، ثم يتم نشر تلك المنصات الخدمية وتوزيعها على عدة نقاط مكانية مـــن أجل ضمان توافر الخدمة (Availability) وبعـــدها تقـــدم للزبـــون الحكومي أو المؤسسي منافذ للإتصال بتلك الخدمات واستخدامها مـــع إعتماد طريقة تسعير حسب الاستهلاك. وبذلك يستريح الزبون كليـــاً من عناء تجهيز وتركيب تلك المنصات البرمجية وضمان توافريتها وتأمين الموارد البشرية اللازمة لإدارتها. ويسمّى هذا النموذج باللغة الانكليزية Platform as a Service.

ومن الأمثلة الواقعية التي يمكن أن تستفيد منها الحكومة في هـــذا النموذج على سبيل المثال هو خدمة SQS من شركة أمـــازون والـــتي تسمح للأنظمة المختلفة بإرسال رسائل فيما بينها حيث تـــؤمن بيئـــة لاتزامنية (Asynchronous) للعمليات الحاسوبية.

البرامج على الطلب (SaaS)

لا تريد مؤسستك أو وزارتك ان تستثمر بالبرمجة مطلقـــاً؟ هـــل تحتاج إلى نظام المحاسبة والإدارة المالية أو شؤون الموظفين على الطلـــب مثلاً؟ إذا هذا هو النموذج الذي أنت بصدد الإستثمار فيه، حيث تعمل الشركات المزودة بتلك النوع من الخدمات على تجهيز برامج متكاملـــة وجاهزة للإستخدام بمجرد الإشتراك معها. ومن الممكن سحب هـــذا النموذج على الحكومة الذكية وإنشاء برامج لمختلف الأعمال الإدارية التي تقوم بها الوزارات والدوائر الرسمية ثم نشر تلـــك الـــبرامج علـــى الكلاود الخاص بالحكومة والطلب من كافة دوائر الحكومـــة الرسميـــة

إستخدامها وبذلك لن يعود هناك حاجة للإستثمار في برامج خدمية متشابهة في كل وزارة على حدة، بل يتم تطوير تلك البرمجيات الحكومية وصيانتها والتأكد من سلامتها مركزياً بينما يتم إستخدامها لامركزياً. وقد تم إطلاق الاسم Software as a Service على هذا النموذج السحابي.

الحكومة على الطلب (GaaS)

سوف تؤدي النماذج الثلاثة السابقة إلى إمكانية تطوير مبدأ "الحكومة على الطلب Government as a Service" حيث تخفي هذه الطبقة الإفتراضية الطبقات الحاسوبية الخدمية الثلاثة وتعقيداتها عن المواطن وأصحاب الأعمال وتمثل بالنسبة لهم في الحكومة الذكية ما كانت تمثله البوابات والبورتال في الحكومة الإلكترونية في العقد الماضي. إن "الحكومة على الطلب" تعني أن الخدمة متوفرة في أي وقت كان وعبر مختلف المنافذ الإلكترونية وقادرة أن تتفاعل مع البشر من خلال واجهات المتصفحات والتطبيقات الذكية وأن تتفاعل مع الآلة من خلال وسائط الإستشعار الحديثة وكل ذلك من أجل خدمة الأهداف السامية التي قامت من أجلها الحكومة وفي مقدمها خدمة مواطنيها والسعي إلى تطوير اقتصاد الدولة وتنمية القطاعات المجتمعية المختلفة وضمان الأمن العام والسيطرة على الخلل الإداري قبل أن يحصل.

الحكومة الذكية الجوّالة

"حتى لو فشلت...يكفيك شرف المحاولة"

الرحّالة ابن بطوطة

الانتشار الكثيف للأجهزة الذكية المحمولة

لقد تغلغلت الهواتف المحمولة بطريقة كبيرة جداً داخـــل معظـــم المجتمعات سواء منها الغربية أو العربية ومع ظهور الجيل الذكي من تلك الأجهزة (الهواتف والأجهزة اللوحية، إلخ...) والذي يمكّن المســـتخدم من الاتصال بشبكة الإنترنت بسهولة وتحميل مختلف أنواع التطبيقات في كافة المجالات ومنها تطبيقات الصحة والحميـــة وتطبيقـــات إدارة الوقت والمحاسبة والألعاب وصولاً إلى تعليم الطبخ وآلاف التطبيقـــات غيرها، بدأ الناس يعتمدون بشكل كبير على تلك الأجهزة وتطبيقاتها في إدارة شؤون حياتهم اليومية وقد تجاوز مستخدمي الإنترنت عبر الهواتف الذكية عدد مستخدميها عبر المتصفحات التقليدية التي تكـــون علـــى أجهزة الكمبيوتر.

هذا الإنتشار والتغلغل في مختلف فئات المجتمع أغرى الحكومـــات حول العالم بإستغلال هذه التكنولوجيا وشجّعها على إطلاق مجموعة من رزمة خدماتها العامة على الأجهزة الجوّالة وأصبح بإمكـــان المـــواطن أن يتواصل خدماتياً مع حكومته بسهولة رفع الهاتف وفتح التطبيق المخصص

لذلك. وقد أصبحت الحكومة الجوّالة (Mobile Government) بصورة جزئية واقعاً عملياً في العديد من البلدان ومنها بعض الدول العربية وهونغ كونغ والهند واستراليا.

الميزات التفاضلية للحكومة الجوّالة

قد يتساءل البعض عن ماهية وجدوى إنتقال الحكومة بهذا الزخم إلى الأجهزة المحمولة سواءً كانت الهواتف الذكية أو الأجهزة اللوحية وفي الحقيقة هناك عدة عوامل تدفع الحكومات بهذا الإتجاه ومنها إمكانية تقديم الخدمة الحكومية حسب البعد المكاني للزبون نظراً لقدرة معظم تلك الأجهزة على تحديد المكان الحالي للمستخدم عبر نظام GPS وما يعني ذلك من إمكانيات كثيرة على مستوى ربط الخدمة الإفتراضية بالأمكنة المادية الفعلية التي تقوم بتسيهل تلك الخدمات وتقديمها وبالتالي بعض العوامل والميزات التفاضلية للحكومة الجوّالة على مثيلاتها من نماذج الحكومة الالكترونية من دون جوّال:

البعد المكاني للخدمة العامة

كما ذكرنا سابقاً تساعد هذه الميزة الحكومة وأجهزتها الخدماتية العاملة على تقديم خدمات مرتبطة بالموقع الجغرافي للمستفيد وعلى سبيل المثال من الممكن تلقائياً إرشاد المواطن إلى أقرب مركز طوارئ طبي أو صيدلية أو مستشفى في نطاق جغرافي صغير بعد التعرف اوتوماتيكياً على مكان ذلك المواطن عبر جهازه المحمول. وينسحب هذا الأمر على الكثير من الخدمات العامة ومنها الأمكنة السياحية ومراكز الشرطة والأمن العام وكل خدمة حكومية تستبطن في داخلها بعداً مكانياً وجغرافياً.

إمكانية التعرّف على الأشياء

وتعني هذه الميزة أن تطبيقات الحكومة الجوّالة سوف تستفيد من أنظمة الأجهزة الذكية التي تساعد في التعرّف على الباركود ومحتـــواه والتعرّف على الوجوه والأمكنة وغيرها من إمكانيات الأجهزة الذكية وعلى سبيل المثال يمكن للمستهلك تمرير جهازه على الباركود الخاص بمنتج إستهلاكي معين من أجل معرفة ما إذا كان أصـــلياً أو مـــزوراً ومعرفة نصائح مصلحة حماية المستهلك حوله فيمـــا إذا تـــوفّرت. أو ببساطة استخدام خاصية الكيوآر كود من أجل الولـــوج مباشـــرة إلى منافذ الخدمة الحكومية عبر تمرير جهازه على تلك الرموز.

الميزة "المحمولية" للخدمة

في أغلب الأحيان لا أحد يتجول في الأسواق او المنتزهات وهـــو يحمل جهازه الكمبيوتر المحمول معه أو يذهب في نـــزهة وهو يتـــأبط ذلك الجهاز تحت ذراعيه، بينما في الهاتف الذكي والأجهـــزة الجوّالـــة يختلف الأمر حيث لا تكاد تبارح تلك الأجهزة حامليها من المـــواطنين حتى عند النوم! وهذا يعني أن الخدمات الحكومية سوف تستفيد هـــذه الميزة "المحمولية" لتلك الأجهزة بحيث تدور الخدمة مع المواطن حيثمـــا دار وترافقه في رحلاته ونـــزهاته وسفراته واعمالـــه. لقـــد جلبـــت الحكومة الالكترونية في العقد الماضي الخدمات العامة إلى مكتب المواطن وجهاز الكمبيوتر الخاص به ولكن الحكومة الجوّالة سوف تضع تلـــك الخدمات الحكومية العامة في جيبة ذلك المواطن.

الخدمات الحكومية الجوالة

كما في الخدمات الحكومية الالكترونية التي انتشرت عبر مواقع الإنترنت، أصبح بالإمكان بناء إطار عمل خدماتي حكومي لأجهزة الجوال والأجهزة المحمولة. ويمكن إنتقاء سلة خدمات عامة من مختلف القطاعات والتي تتمحور حول حاجة المواطن اليومية من المعلومات والمعاملات الحكومية وتقديمها عبر مجموعة من التطبيقات الذكية ودعمها بخدمات إلكترونية حكومية مشتركة مثل أنظمة تسديد الرسوم عبر الجوال والتأكد من هوية المستخدم ويبين لنا الجدول التالي نماذج عن تلك الخدمات الحكومية الجوالة في بعض القطاعات:

القطاع الحكومي	تطبيقات محتملة وأمثلة
حماية المستهلك والملكية الفكرية	تطبيق مؤشر الأسعار للمستهلك تطبيق البحث عن براءات الإختراع والمواد المتعلقة بالعلامات المسجلة وغيرها تطبيق البحث عن البضاعة الغير أصلية وتمييزها عن الأصلية في السوق تطبيق إرشادات توعية للمستهلكين
القطاع الزراعي والحيواني	تطبيق خاص بأمراض المواشي وكيفية رعايتها تطبيق المواسم الزراعية ومعلومات عن كل رراعة وسبل تنميتها والمواد الكيميائية المخصصة لحماية المنتوج تطبيق دليل المزارعين والتجار
القطاع الإداري الحكومي	تطبيق تعقب ومتابعة المعاملات الرسمية تطبيق تسديد الرسوم الحكومية على اختلافها (محاضر ضبط، مخالفات، ...) تطبيق الوظائف المتوفرة في القطاع الحكومي تطبيق الشكاوى والمراجعات

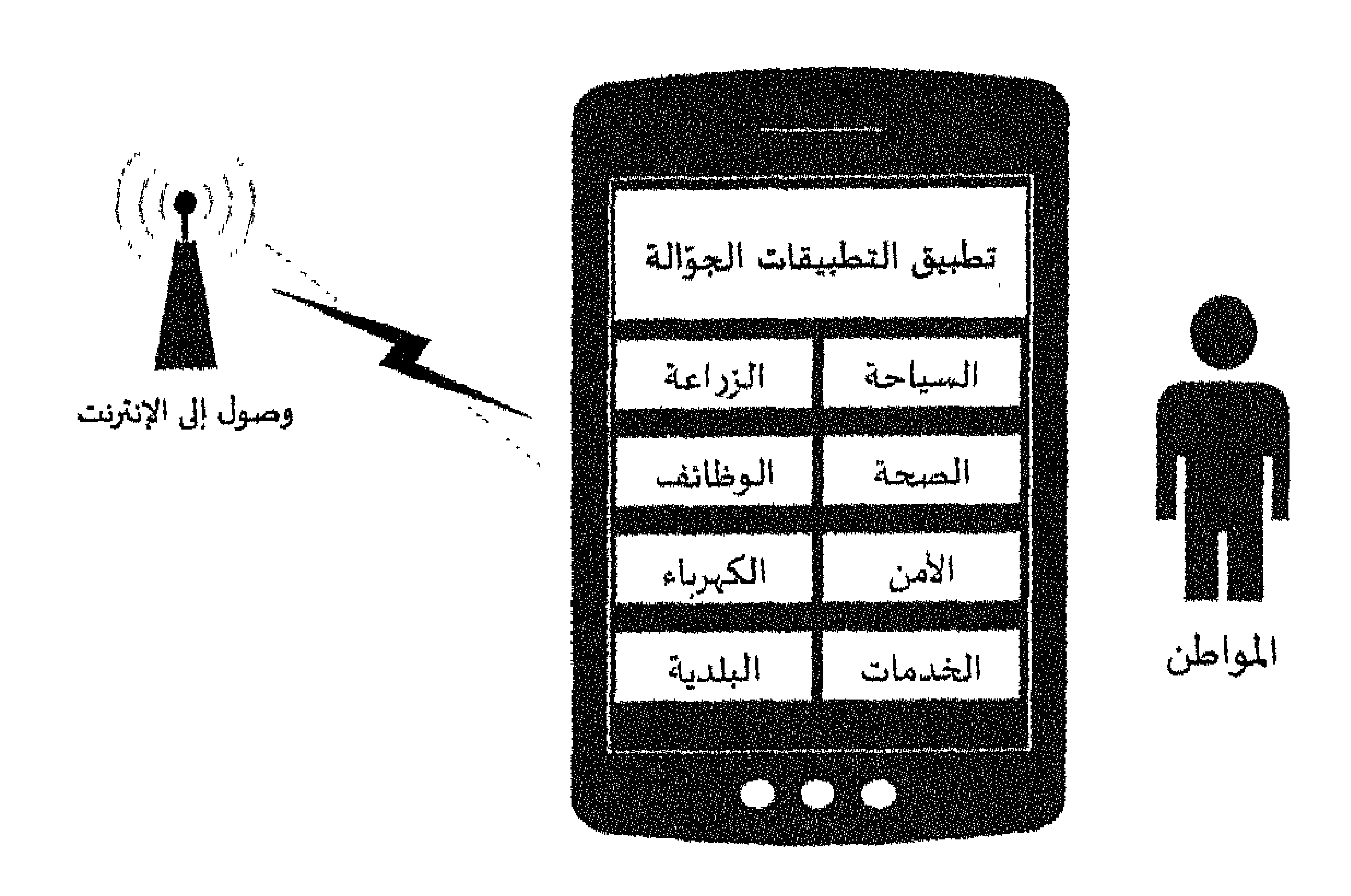
	تطبيق إداري خاص بوضع الموظف الحكومي (إجازات، مستحقات مالية، قروض،)
القطاع الصحي والرعائي	تطبيق الارشادات العامة والوقائية في مجال الصحة تطبيق ملف المريض الصحي (التاريخ الصحي، الأدوية التي يتعاطاها، فئة الدم، ومعلومات أخرى تساعد الطبيب مباشرة على معرفة طبيعة المريض الذي يتعامل معه) تطبيق الرعاية الأولية والإجراءات الخاصة بالإسعافات الأولية تطبيق دليل المستشفيات والصيدليات في الدولة وكيفية الوصول اليها عبر الخرائط الالكترونية
القطاع المالي والمصرفي	تطبيق البنوك والمؤسسات المالية المرخّصة في الدولة
القطاع التعليمي	تطبيق دليل الجامعات والمعاهد والمدارس تطبيق نتائج الإمتحانات الرسمية تطبيقات تعليمية مختلفة للطلاب
القطاع السياحي	تطبيق الأماكن السياحية المهمة في الدولة وإرشادات حول كيفية الوصول اليها ورسومها المالية وأوقات عملها تطبيق دليل المطاعم السياحية والفنادق والمنتجعات حسب المناطق
تطبيقات خدمية مختلفة	تطبيق الإشعارات الحكومية (فعاليات، مؤتمرات، وكل ما يتعلق بالعمل الحكومي من نشاطات) تطبيق خاص بالمستثمرين الاجانب وكيفية الاستثمار في الدولة وشروطه تطبيقات خاصة بالأمن العام ودائرة الهجرة حول مختلف خدماته مثل الحصول على تأشيرات الدخول والإقامة والعمل تطبيق المكتبات العامة تطبيق حركة النقل العامة واوقات الباصات والتراماواي وغيرها من وسائل النقل العام تطبيق حركة الطيران في المطارات العاملة في الدولة

جدول 4: أمثلة التطبيقات الذكية في الحكومة الجوّالة

يحتوي الجدول السابق على أمثلة عن التطبيقات الذكية التي يمكن بناؤها من أجل خدمة المواطن وقطاع الأعمال بطريقة أفضل ومتوفرة على مدار الساعة ويوجد الكثير من التطبيقات التي يمكن إضافتها إلى تلك اللائحة بعد دراسة عملية لوضع كل حكومة ومعرفة أولوياتها الحكومية ومواردها المالية والبشرية المؤهلة لتنفيذ تلك التطبيقات وحماية أمنها وخصوصية معلوماتها.

تطبيق التطبيقات الذكية

كما لاحظنا سابقاً، فإن عدد التطبيقات الحكومية الذكية قد يصبح كبيراً وبالتالي يضع المواطن أمام معضلة إيجاد الخدمة الحكومية التي يريدها بسهولة وقد تمكنت الحكومة الالكترونية في العقد الماضي من حل تلك المعضلة إلى حد كبير عبر تركيب الخدمات حول حاجات المواطن وليس الدوائر الحكومية ولكن حجم الأجهزة الجوالة وصغر شاشاتها يفرض المزيد من التحديات في هذا المجال ولذلك فقد قامت العديد من الدول التي استثمرت بتكنولوجيا الحكومة الجوالة ببناء تطبيق موحّد مركزي يكون بمثابة بوابة للتطبيقات الأخرى في مختلف المجالات وبذلك فهي حافظت على مركزية البحث عن الخدمة الحكومية بينما تركت الحرية للوزارات والدوائر الرسمية ببناء تطبيقاتها الخاصة وفقاً لما تراه مناسباً.



رسم توضيحي 6: تطبيق التطبيقات الذكية

ويحتوي "تطبيق التطبيقات الذكية" على لائحة منظّمة بالتطبيقات الحكومية ويضمن أن التطبيقات التي يتم الدخول اليها من خلال التطبيق المركزي هي تطبيقات شرعية تم نشرها من قبل جهة حكومية وليست تطبيقاً وهمياً على مخزن التطبيقات العامة.

الرزمة التوجيهية لتطبيقات الحكومة الجوالة

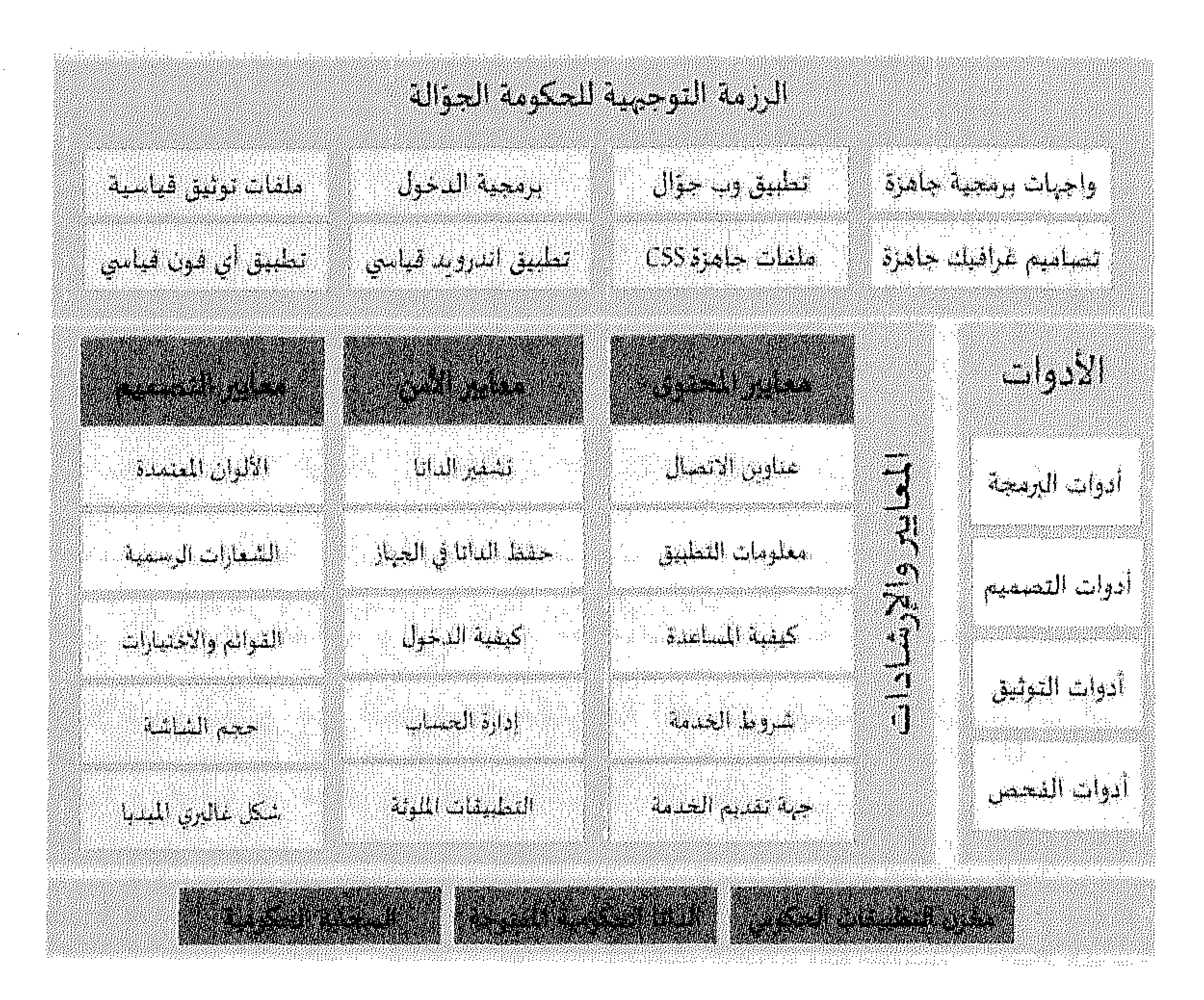
سوف يؤدي إطلاق يد الوزارات والإدارات العامة في تطوير تطبيقات جوالة خاصة بخدماتها الحكومية إلى إنتاج خليط غير متجانس من تلك التطبيقات قد تؤدي إلى تضليل المواطن أو تشتيت عملية معاملاته مع الخدمات الحكومية الجوّالة وذلك لأسباب تتعلق بعدم توحيد تلك التطبيقات على صعيد المظهر من ألوان وتصاميم وشعارات وعلى صعيد المضمون العام مثل إمكانية البحث وترويسة التطبيق وتذييله والعلامات التجارية او المضمون الخاص المتعلق بالخدمات الحكومية بذاتها. وبناءً عليه من المهم أن تعمد الحكومة المركزية إلى

تحضير "رزمة توجيهية" من الإرشادات والمقاييس التي ينبغي على التطبيقات الجوالة التقيد بها من أجل الموافقة على نشرها في مخزن التطبيقات الحكومية وجعلها متوفرة للعامة.

وتعالج تلك "الرزمة التوجيهية" المقاييس والمعايير التالية على سبيل المثال:

- المحتوى العام للتطبيق: وهو المحتوى الذي يظهر في جميع التطبيقات الحكومية الجوّالة من قبيل: نسخة إصدار التطبيق ومعلومات عنه ومعلومات الجهة المقدمة للخدمة وكيفية الإتصال بها وبيان الخصوصية المشترك مع الدوائر الأخرى وبيان إخلاء المسؤولية.
- المحتوى الخاص للتطبيق: وهي معلومات الخدمة المقدّمة ومتطلباتها وعملية تنفيذها الفعلي والحقول المطلوبة للتعبئة قبل إرسال طلب الخدمة إلكترونياً.
- معايير التصاميم والألوان: وهي مجموعة المعايير الغرافيكية والجمالية التي يجب على مختلف الدوائر الإلتزام بها عند بناء تطبيقات حكومية جوالة.
- معايير أمن الخدمة: سواءً كانت الخدمة تحتاج إلى عملية تشفير أثناء نقل الداتا من المحمول إلى خوادم الدولة او سحابتها الحاسوبية وايضاً معرفة حساسية الداتا المحفوظة في الجهاز وما إذا كانت تستدعي تشفيراً داخل الجهاز حتى لا يتم كشف كل الداتا الحسّاسة إذا ضاع الجهاز أو سرق.
- شكل القوائم (Menus) والصفحة الترويجية الأولى للتطبيق (Splash Screen) ومحتويات قائمة الإعدادات الخاصة بالتطبيق.

- كيفية دعم أحجام الشاشات المختلفة والمقاسات المفضلة وكيفية إظهار التطبيق في الوضع الأفقي أو الوضع العامودي للجهاز.



رسم توضيحي 7: الرزمة التوجيهية لتطبيقات الحكومة الجوّالة

سوف تساعد الإرشادات التوجيهية والمعايير المختلفة على إنتاج مجموعة متناسقة من التطبيقات الحكومية الجوالة وتساهم في تخفيض كلفة التطوير وخاصة أثناء المرحلة الأولية لتصميم التطبيق ومحتوياته. ومن الممكن أخذ هذا المفهوم خطوة إلى الأمام عبر بناء مجموعة تطبيقات قياسية تتضمن العمود الفقري لأي تطبيق حكومي مع تصاميمها وجعلها متوفرة بين أيدي المبرمجين مع شيفرتها البرمجية الكاملة من أجل البناء عليها (mGovernment Toolkit).

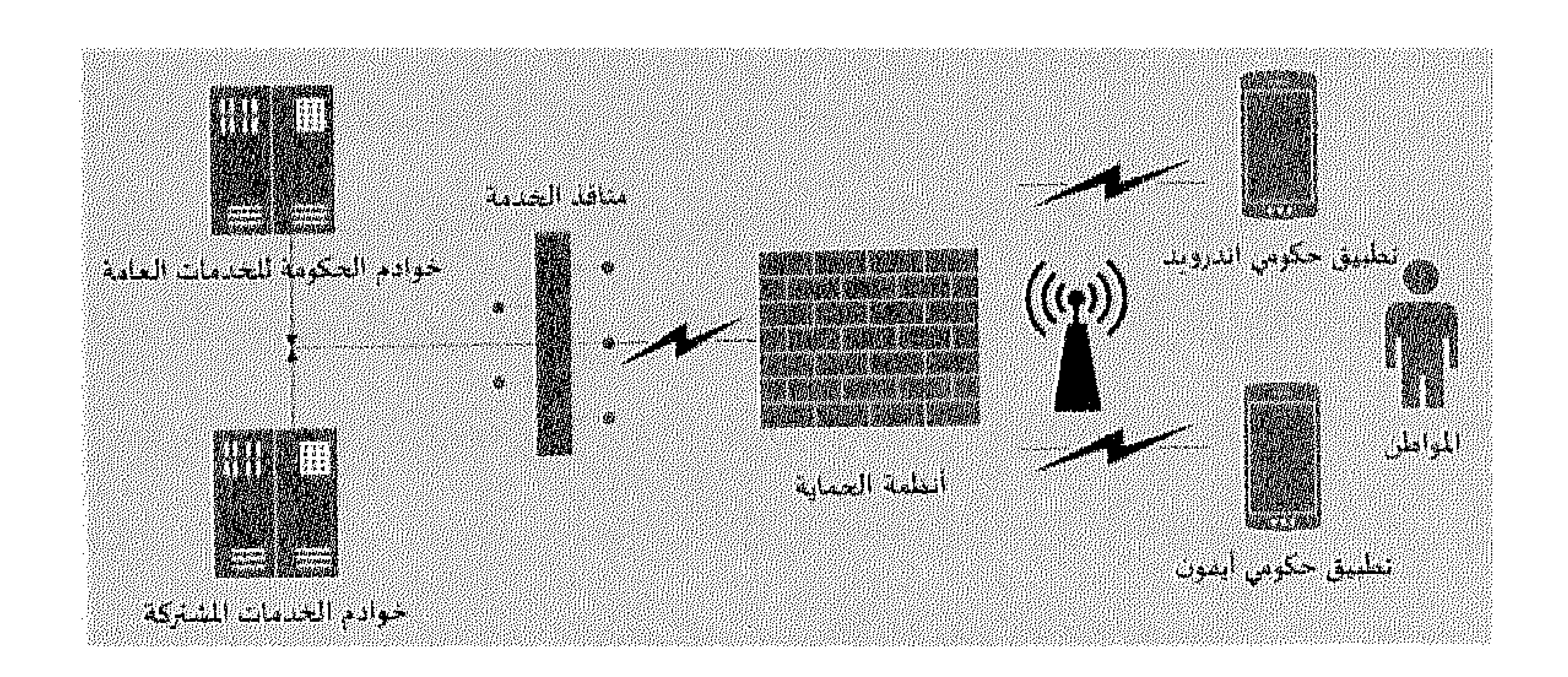
واجهة الإنترنت البرمجية للتطبيقات الذكية

في أغلب الأحيان تحتاج تطبيقات الجوّال الحكومية إلى أن تتواصل مع أنظمة وخوادم الحكومة من أجل سحب الداتا المطلوبة أو إرسال الداتا التي يقوم بتعبئتها المواطن أو التأكد من هوية المستخدم قبل دخوله إلى التطبيق وبداية التفاعل معه. وعلى سبيل المثال يحتاج تطبيق البحث عن العلامات التجارية إلى منفذ برمجي (API endpoint) على الشبكة الحكومية حيث يتم إرسال كلمات البحث من التطبيق إلى الجوّال إلى ذلك المنفذ والذي يتواصل مع الأنظمة الخلفية للحكومة من أجل جلب النتائج وإرسالها مجدداً إلى طالب الخدمة. ويطلق على هذه مجموعة هذه المنافذ إسم (Web API) وقد إنتشرت مؤخراً مجموعات كبيرة من تلك الأنظمة الخدمية والتي تقدم خدمات مناخية وأسعار صرف عملات والكثير من المعلومات مفتوحة المصدر عبر الإشتراك بها بصورة مجانية أو مدفوعة للخدمات الأكثر تقدماً.

ولا تستطيع الحكومة الجوّالة أن تكون ناجحة تماماً من دون رسم وتطبيق إطار مرجعي يعالج منافذ الخدمات الحكومية على إختلافها ويسهل على المبرمجين عملية التواصل مع تلك الخدمات واستخدامها. وسوف يعالج الإطار المرجعي لواجهة الإنترنت البرمجية للحكومة مسائل تتعلق بكيفية إستخدام تلك المنافذ ومجموعة من الأمور التالية:

- كيفية تسجيل الدخول من أجل إجراء عمليات تواصل مع تلك المنافذ والإطار التقني الأهم في هذا المجال هو oAuth
- حجم الإتصال اليومي المسموح لكل مبرمج حتى لا يتم إغراق أنظمة الحكومة بالكثير من العمليات (API daily rate)
- كيفية توليد المفاتيح السرية للإتصال البرمجي ومعها معرّف الزبون (Client Id and API secret key)

- عنوان المنفذ على الشبكة
- بروتوكول التواصل التقني ونسق الداتا الذاهبة من الزبون والقادمة من سيرفيرات الحكومة (HTTP, SSL, JSON,)



رسم توضيحي 8: منافذ الخدمات البرمجية للتطبيقات الذكية

وقد تكون منافذ الخدمات الجوّالة البرمجية موزّعة على مختلف الإدارات أو مركزية في السحابة الحاسوبية الحكومية ويفيد كتاج منشور عن تلك المنافذ ومواصفاتها التقنية في عملية تطوير البرمجيات الجوّالة الخاصة بالحكومة الذكية.

أمن التطبيقات الذكية

في حالة تطبيقات الوب ومواقع الحكومة الالكترونية كان بالإمكان أن يتم حماية تلك التطبيقات مركزياً مع شيفرتها البرمجية حيث لا يتم توزيع تلك التطبيقات بل يتعامل معها المستخدم من خلال المتصفحات، ولكن الحال تختلف بالنسبة لتطبيقات الجوّال السميكة (Native thick client apps) والتي يتم تحميلها على الجهاز الجوّال نفسه مما يفتح المجال امام الهاكرز وغيرهم، في كثير من الأحيان،

لتحميل التطبيق وإعادة إنتاج الشيفرة البرمجية منه أو الحصول على تفاصيل تقنية حول كيفية ومكان تخزين الداتا في الجهاز مع إمكانية الحصول على نسخة منها. وعلى صعيد آخر، تكون الأجهزة الجوّالة معرّضة للسرقة أو الضياع أو البيع من دون أخذ الاحتياطات اللازمة وإزالة الداتا الشخصية عن تلك الأجهزة.

ولا يمكن الإعتماد على المواطن مطلقاً في حماية التطبيقات الذكية التي يقوم بتحميلها من مخزن تطبيقات الحكومة الجوّالة بل يجب على فريق التطوير أن يعمل على تضمين وسائل الأمان وسرية المعلومات داخل تطبيقاتهم. وعلى سبيل المثال، عندما يحتاج التطبيق الذكي في مجال الصحة العامة إلى حفظ داتا المواطن محلياً فإنه يجب الأخذ بعين الإعتبار إمكانية وقوع الجهاز بين أيدي غير أمينة تتلاعب بتلك الداتا وتحصل عليها او تنشرها وما إلى هنالك وفي هذه الحالة من الممكن أن تفرض الحكومة الذكية معايير تشفير الداتا في المخازن المحلية للأجهزة الذكية وفك تشفيرها فقط خلال تظهيرها وقراءتها من داخل التطبيق.

ولا تقتصر المخاطر الأمنية للأجهزة الجوّالة على إساءة إستخدامها بل من الممكن أن يقوم المستخدم وعن غير معرفة بتحميل برامج ملوّثة (Malware) على نفس الجهاز حيث تقوم تلك البرامج بسرقة كلمات دخوله إلى تطبيقات الحكومة الجوّالة أو إستخدام محفظة نقوده الجوّالة (m-payment system) من أجل سرقة أمواله أو ببساطة إرسال رسائل من دون معرفة ذلك المواطن.

ونظراً لعدم إمكانية التحكم مركزياً بأجهزة المواطنين الجوّالة، فإن المعالجة الأمنية للتطبيقات الذكية الحكومية تتفرع إلى عدة فروع وهي:

- المعالجة التقنية لأمن التطبيقات: وتشمل وسائل تشفير الداتا في المخازن المحلية للأجهزة الجوّالة وتشفير الداتا خلال طريقها

من الجهاز وإلى خوادم الحكومة (SSL traffic) وإعتماد برامج تمنع من إعادة إنتاج الكود البرمجي لتلك التطبيقات وتسجيل آثار العمليات الالكترونية (Audit Log).

- إشعارات العمليات المهمة: عندما يقوم التطبيق بإجراء عملية مهمة مثل تسديد الرسوم أو إجراءات عمليات سرية ينبغي إشعار المواطن من خلال رسائل خاصة حتى يتمكن من معرفة ما إذا كانت هناك برامج ملوّثة تقوم بتلك العمليات من غير علمه وفي هذه الحالة يقوم المواطن بالإبلاغ عن تلك العمليات من أجل معالجتها مركزياً وإتخاذ الإجراءات اللازمة.
- تطبيق عوامل إضافية للتأكد من الهوية: في التطبيقات الأكثر حساسية أمنياً، من الممكن أن تقوم الحكومة بالتأكد من هوية المستخدم عبر تطبيق أكثر عامل على عملية الدخول (Multi-factor authentication)، مثلاً بالإضافة إلى كلمة السر يطلب التطبيق مسح بيومتري أو إدخال شيفرة يتم تحديثها دورياً.
- إجراءات إلغاء تفعيل الأجهزة المسروقة: ماذا تفعل دائرة التطبيقات الجوّالة في الحكومة الذكية إذا تم الإبلاغ عن سرقة جهاز جوّال يحتوي على معلومات الدخول الخاصة بالمواطن؟ وكيف تقوم بإلغاء تفعيل حسابه وإلى ما هنالك من إجراءات.
- التوعية الأمنية للمبرمجين: تدريب مبرمجي التطبيقات الجوّالة على مجموعة المعايير الأمنية التي يجب الإلتزام بها من أجل السماح لهم بنشر تطبيقات حكومية ذكية.

وإضافة على ما تقدم، يجب العمل على تـأمين الجهـة الخلفيـة للتطبيقات الذكية والتأكد من ضمان أمن الداتا فيها وسلامتها.

نموذج مرجعي: تطبيق البرلمان الالكتروني الذكي

من أجل توضيح موضوع المنافذ الحكوميـة الإلكترونيـة علـى الإنترنت سوف نقدم مثالاً عملياً عن تطبيق البرلمان الإلكتروني الذكي وكيفية بناء منفذ على الإنترنت من أجل خدمة الـداتا وإيصـالها إلى المستفيدين، ومن اجل إختصار المتطلبات الوظيفية للتطبيـق سـوف نفترض ان تطبيق االبرلمان الإلكتروني الذكي سـوف يحتـوي علـى الوظائف التالية:

1. تسجيل الدخول والخروج عبر اسم المستخدم وكلمة السر
2. إستعراض أسماء النواب ومعلومـاتهم الشخصـية وكيفيـة الإتصال بهم
3. البحث عن قرارات ومشاريع مجلس النواب
4. مشاهدة مقاطع فيديو مسجلة من الجلسات العامة
5. إرسال الملاحظات والتعليقات إلى الجهة المعنية في البرلمان

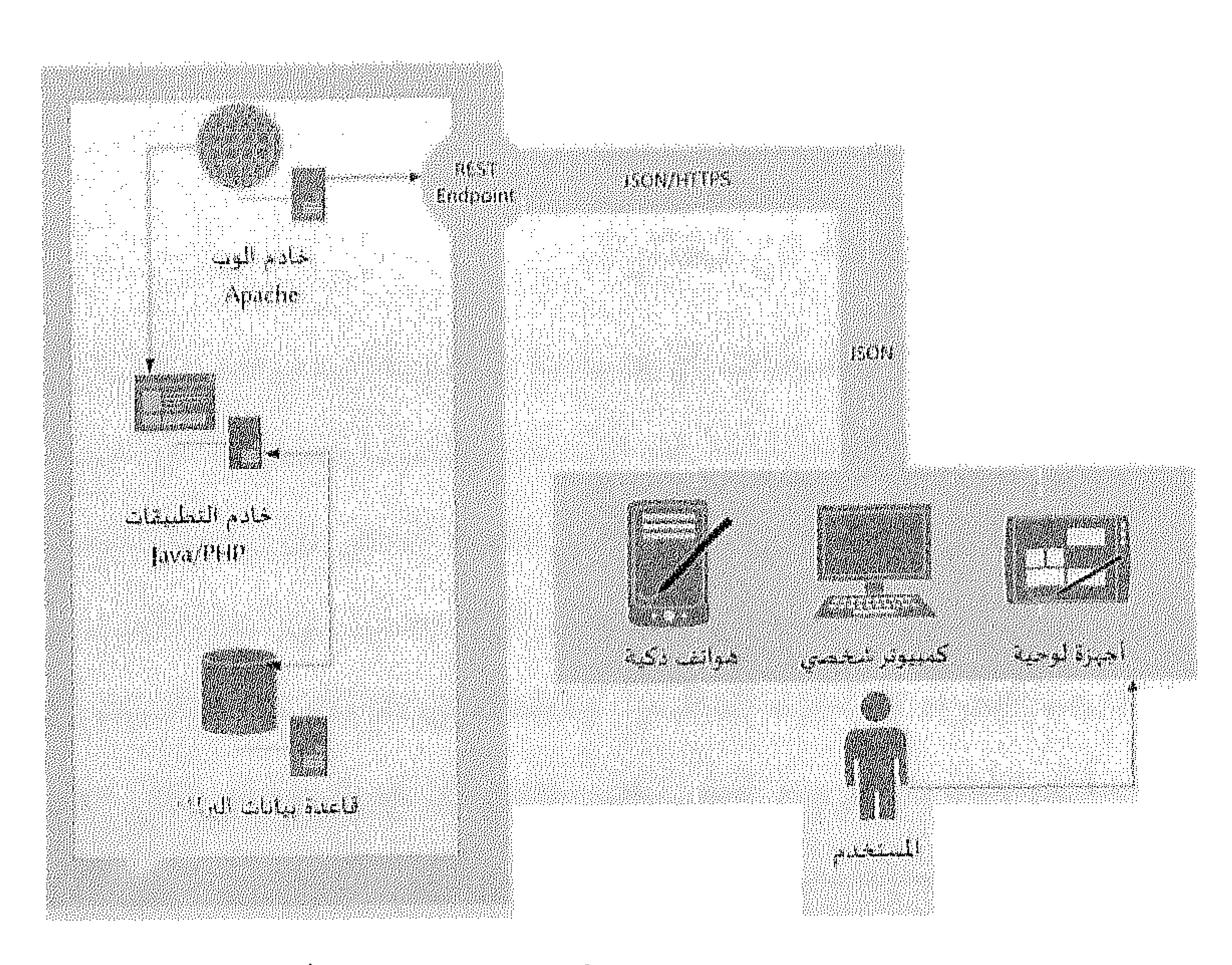
وكما قلنا سوف نكتفي بالوظائف أعلاه والهدف هنا هو لـيس بناء تطبيق متكامل بل شرح كيفية مقاربة المشروع وإختيار المكونـات البرمجية اللازمة وشرح عملية الاتصال بين الجهاز الذكي ومنافذ البرلمان الإلكترونية على الإنترنت.

معمارية تطبيق البرلمان الالكتروني

سوف يتم تقسيم التطبيق إلى قسمين رئيسيين وهمـا: التطبيـق الجوّال على أنظمة أندرويد أو آي فون أو بلاكبيري والذي سوف يمثل

الواجهة التطبيقية والاستخدامية للمواطن وعبرها سوف يتفاعـــل مـــع الخدمة البرلمانية الالكترونية والقسم الثاني هو الواجهة الخلفية للتطبيـــق وتمثل منفذ الإنترنت (Parliament WEB API) وخادم الوب وقاعدة البيانات ونظام الحماية والنظام الخلفي المسؤول عـــن تخـــديم الـــداتا واستقبال التعليقات والملاحظات.

ويوضح لنا النموذج التالي معمارية تطبيق البرلمـــان الإلكتـــروني بشقيه المذكورين أعلاه:



رسم توضيحي 9: معمارية تطبيق البرلمان الذكي

ويقوم منفذ الإنترنت الموضّح أعلاه تحت إسم (REST Endpoint) بإستقبال طلبات الداتا من الأجهزة المختلفـــة والتأكـــد مـــن أهليـــة ومشروعية المتصل ثم التواصل مع خادم التطبيقات من أجـــل تنفيـــذ الطلب الإلكتروني والذي بدورع يقوم بسحب الداتا من قاعدة بيانات

البرلمان ثم تحويلها إلى النسق القياسي (JSON) وبعدها إرسـالها عـبر نفس المنفذ إلى المتصل والذي قد يكون جهاز هاتف ذكي أو كمبيوتر شخصي أو جهاز لوحي ومن المعلوم أن النسق (JSON) هو نسق داتا خام ولا يحمل في تركيبته أية معلومات عـن كيفيـة عـرض الـداتا وتظهيرها على تلك الأجهزة حيث تكون مسـؤولية عـرض الـداتا البرلمانية مسؤولية مبرمجي تلك التطبيقات.

الحكومة الذكية الإجتماعية

"الثمن الذي يدفعه الطيبون لقاء عدم مبالاتهم بالشؤون العامة هو أن يحكمهم الأشرار"

أفلاطون

هل يمكن للحكومة أن تختار؟

لا شك بان الشبكات الإجتماعية والمدونات ومواقع مشاركة الفيديو والنصائح والتعليقات قد شهدت تطوراً مذهلاً في عدد مستخدميها في السنوات الماضية حتى ذهب البعض إلى تحميل تلك المنصات الإلكترونية مسؤولية الثورات التي حدثت في العالم العربي وربما هم محقون في الجزء التنظيمي والتحفيزي من ذلك وليس في الأسباب الجذرية لخروج الناس على بعض الأنظمة. وعلى كل حال، فقد بلغ عدد مستخدمي الفايسبوك وحده أكثر من مليار مستخدم حتى العام 2013، بينما يبلغ عدد مشاهدات اليوتيوب حوالي ست مليارات ساعة مشاهدة كل شهر ناهيك عن التويتر وانستغرام وبنترست وغيرها. وتؤشر هذه الهجرة الإفتراضية إلى المجتمع الرقمي أن الناس بدأت تعتاد على ذلك النموذج وبالرغم من أنه وردت تقارير بتاريخ كتابة هذا الكتاب ومنها دراسة مجموعة باحثين من جامعة برنستون يتوقعون فيها أن يفقد الفايسبوك حوالي 80 % من

مستخدميه بحلول العام 2017 فإن هذا لا يعني العودة مجدداً إلى المجتمع المادي من الفايسبوك بل على العكس من ذلك سوف تكون أي هجرة للمستخدمين من الفايسبوك مؤشراً على ولادة شبكات إجتماعية أكثر نضجاً وتفهماً لحاجات المستخدمين وخصوصية معلوماتهم وأمنهم الشخصي. لقد إعتاد المواطن على "النموذج" وليس على الفايسبوك وهو بالذات ما سوف يستمر حتى لو تغير الفايسبوك أو التويتر.

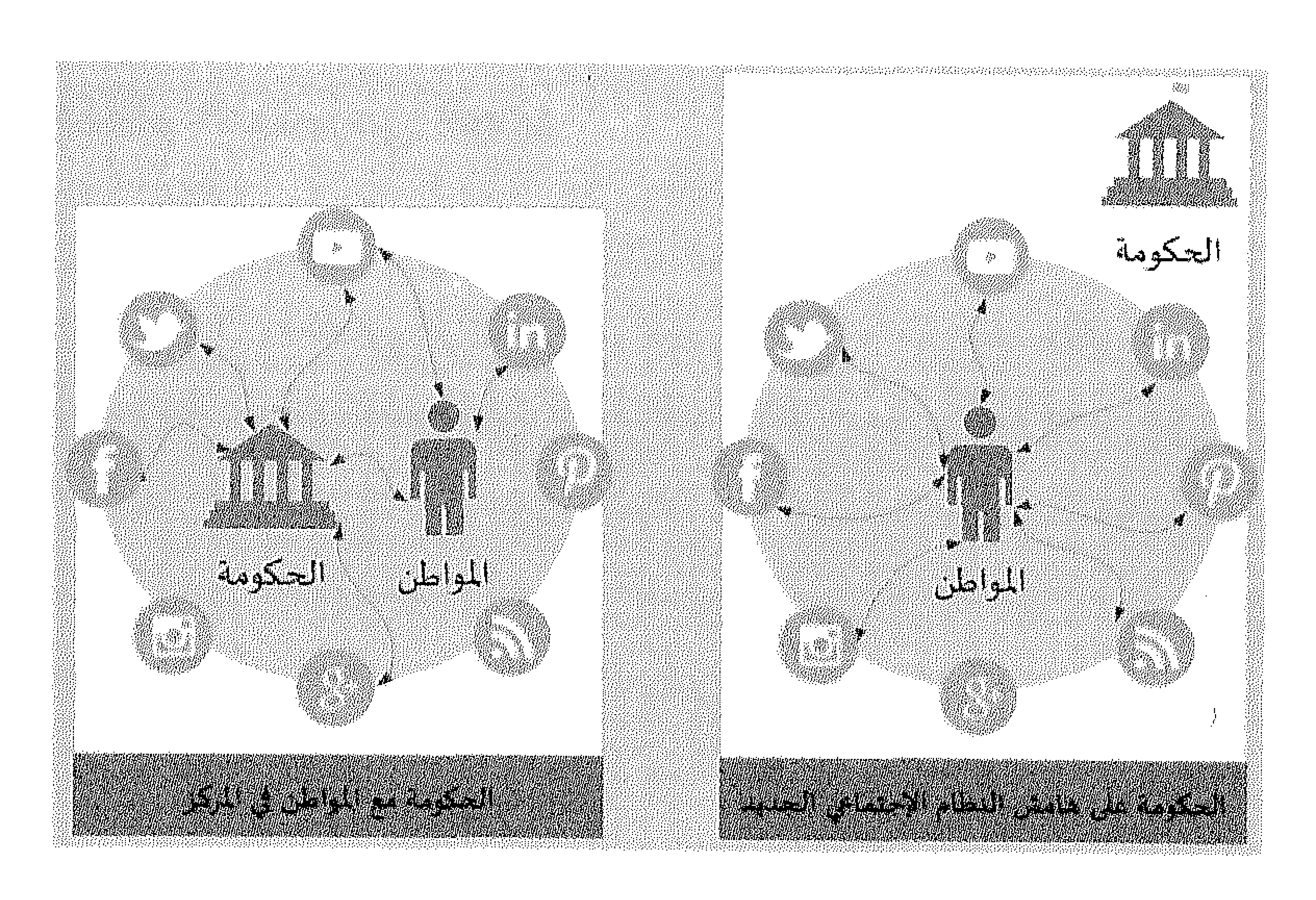
في ظل هذه التغيرات في سلوكيات المواطنين وكيفية تواصلهم داخلياً وخارجياً وتركيبة شبكاتهم والطريقة التي يتلقون فيها المعلومات ويشاركون فيها بالتعليقات هل يمكن للحكومة أن تختار وتبقى خارج النظام الاجتماعي الالكتروني العالمي الجديد؟ هل يمكن للحكومة أن تغض النظر عن الأدوات الإتصالية الحديثة حيث يعيش معظم مواطنيها حياتهم الإفتراضية فيها؟ وهل سوف يبقى لأي حكومة تأثير على شعبها ما لم تستطع أن تخاطبهم بالطريقة التي يفهمونها؟

لقد سبق الإعلام والفضائيات في العقد الماضي معظم الحكومات إلى الفضاء بينما بقيت تلك الحكومات على الأرض وقد تعلمت الدرس غالياً حينما استفاقت تلك الحكومات على وسائل إعلام فضائية أكثر تأثيراً بمواطنيها من وسائل إعلامها المحلية، واليوم أيضاً يتكرر الشيء نفسه مع الشبكات الإجتماعية الإلكترونية "النموذج" الجديد للتواصل وإذا لم تستطع الحكومة تطوير كوادرها ووضع سياسات واضحة وسريعة لكيفية النشاط الحكومة الإجتماعي الإلكتروني فسوف تستفيق مجدداً على صدمة من نوع آخر! صدمة إلكترونية إجتماعية تجد نفسها فيها الأقل تأثيراً وصدقيةً وشفافيةً من أي مكوّن إجتماعي أمام مواطنيها.

النظام الإجتماعي الجديد

من الواضح أن النظام الإجتماعي لفئات الشباب والمراهقين قد شهد تحولاً يستدعي مراقبته عن كثب حيث بدأت تتشكل أنظمة إجتماعية حديثة تعتمد على الصداقات الإفتراضية والمجموعات التي يتم تركيبها من تلك الصداقات بالإضافة إلى أنماط جديدة في التواصل يتم التعبير عنها بالتعليقات والتدوين السريع ومشاركة الصور ومقاطع الفيديو والأعمال الغرافيكية التي تعكس الوضع السياسي أو الأمني أو الإقتصادي مسحوباً على كل مجالات الحياة.

ومن أجل ان تكون إجتماعياً في الحياة الإفتراضية أصبح عليك أن تكون منعزلاً في الحياة الواقعية مما يعني أن الأفكار الفردية والمعتقدات الشخصية والرأي العام في المجتمع قد أصبحوا جميعاً يتأثرون بطريقة أو بأخرى بما يحدث في الشبكات الإلكترونية الإجتماعية والتي برعت في طريقة تقديم الأصدقاء الجدد عبر خوارزميات معقّدة تدرس الإهتمامات الفردية وعلاقات المستخدم وشبكة مجموعاته والتعليقات التي يقوم بنشرها من أجل دفع المستخدم لتوسيع دائرة علاقاته وأصدقائه الإفتراضيين وبالتالي يستمر "النموذج" الإجتماعي الجديد بالحياة عبر ضخ دماء جديدة فيه بطريقة سهلة.



رسم توضيحي 10: الحكومة في النظام الإجتماعي الإلكتروني

وبما أن هذا الكتاب ليس بحثاً إجتماعياً متخصصاً نكتفي بالقول بأن الحكومة مهما كان شكلها أو مكانها أو بلدها عليها أن تتماشى مع النظام الإجتماعي الجديد إذا كانت جدية في عملية الحكم وتطوير الدولة والبقاء على قرب من مصدر التشريع الأساسي ألا وهو المواطن. إنه النظام العالمي الإجتماعي الجديد وعلى الحكومة ان تختار إما ان تكون على الهامش وتابعة دائماً أو تكون في قلب ذلك النظام تؤثر فيه وتتطور به وتحافظ على وجودها في العالم الإفتراضي كما في العالم الواقعي.

الإستراتيجية الحكومية للشبكات الإجتماعية

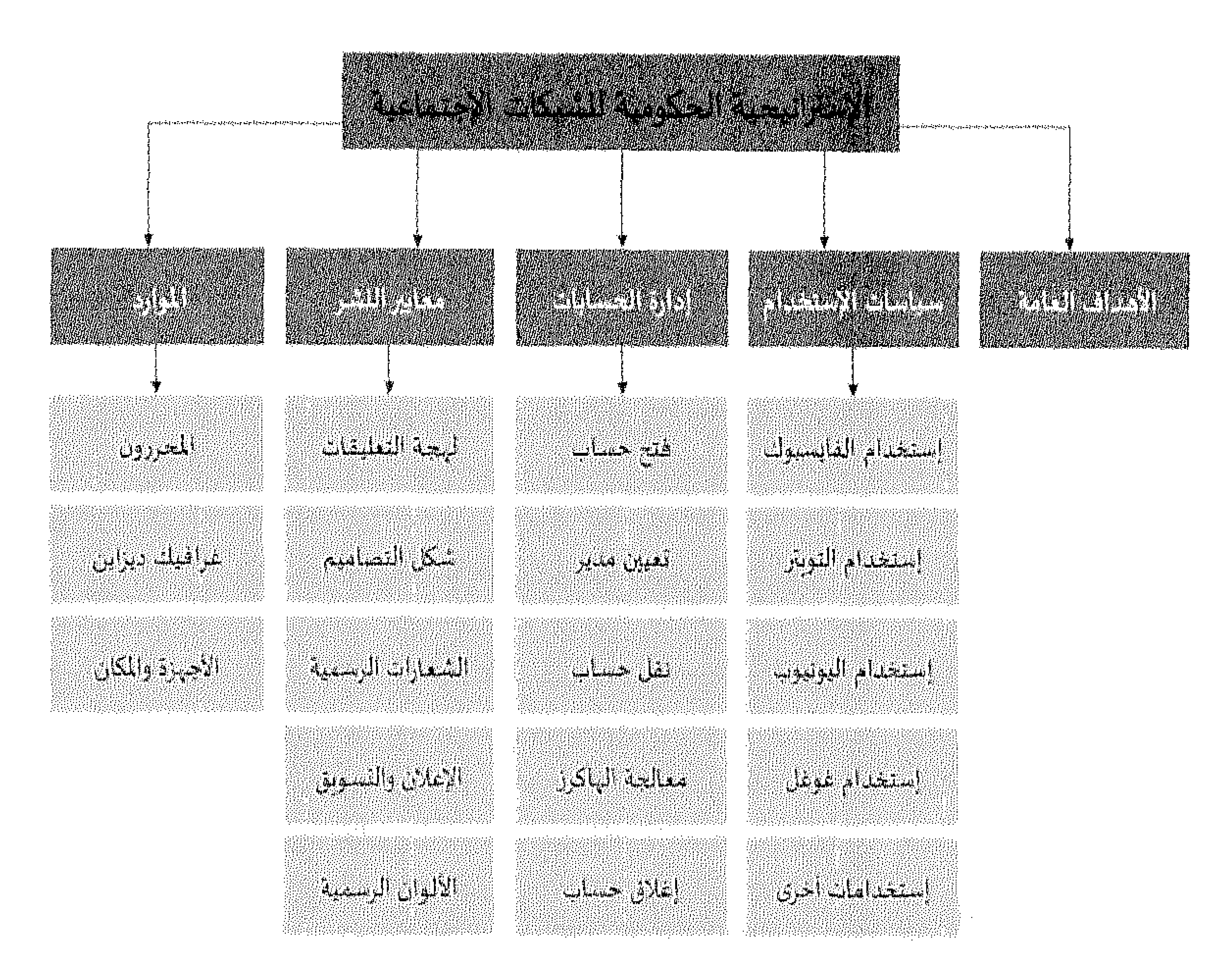
قرّرت الحكومة أن المشاركة في الحراك الالكتروني الإجتماعي هو مصلحة عامة ولا بد من مقاربة هذا الموضوع بطريقة ذكية وآمنة، الآن ماذا؟ نعتقد أنه قبل إندفاع الحكومة ومشاركتها بالشبكات الإجتماعية

الإلكترونية بطريقة عشوائية قد تؤذي صورها العامة بدلاً من تحسينها يجب العمل على تطوير "إستراتيجية إلكترونية إجتماعية" تبين الاهداف العامة للحكومة في هذا المجال ومجموعة سياسات الإستخدام الحكومي لتلك المنصات وكيفية إدارة الحسابات الإجتماعية الرسمية على الشبكات مثل فايسبوك وتويتر ويوتيوب ومن هم الأشخاص المخولون بالنشر على تلك الصفحات.

وقد تحتوي تلك الإستراتيجية الحكومة الإلكترو-إجتماعية على العناوين التالية:

- إدارة عملية فتح الحسابات الإجتماعية الحكومية ومن هي الجهة المخوّلة بتلك العملية من بداية إختيار الشبكة الإجتماعية وإختيار إسم الحساب وتعيين مدير للحساب ووصولاً إلى إغلاق ذلك الحساب في حال الضرورة.
- الإجراءات العملية في حال تم إختراق أحد الحسابات الإلكترونية الحكومية من قبل الهاكرز الذين قد يعمدون إلى نشر معلومات لتضليل الرأي العام.
- الموارد البشرية والمادية المتوفرة لإدارة عملية التواصل الإجتماعي-الحكومي على الإنترنت.
- إعتماد مركزية النشر الإلكتروني الحكومي عبر جهاز الحكومة الذكية البشري بدلاً من بعثرة هذا الموضوع على الوزارات والإدارات العامة وننصح بهذا النموذج خاصة في الدول النامية حتى يتم التأكد من جودة المعلومات المنشورة مركزياً وجودة الإعمال الغرافيكية والصور ومقاطع الفيديو وخلوها من أية مواقف قد تضع الحكومة تحت الحرج.

- تحديد الشبكات الإجتماعية الفعّالة بشكل دوري وإعتماد الأكثر إنتشاراً منها على الصعيد المحلي.
- تطوير ونشر وثيقة المعايير الخاصة بجودة المعلومات الإجتماعية وألوان وتصاميم الأعمال الغرافيكية الحكومية ومقاييس الصور والشعارات الرسمية الواجب إستخدامها دون غيرها على الشبكات الإجتماعية.



رسم توضيحي 11: الإستراتيجية الحكومية للشبكات الإجتماعية

ومن المهم التمييز بين الحسابات الشخصية التابعة للوزراء على سبيل المثال وبين الحسابات الإلكترونية التابعة للحكومة حيث تبقى تلك الحسابات بعهدة الوزارات والأجهزة ولا علاقة لها بمجيء وزير جديد أو ذهابه.

الأدوات والشبكات الإجتماعية الالكترونية

في معرض الحديث عن الحكومة الإجتماعية لا بد من التطرق إلى الأدوات والمنصّات المتوفرة حالياً في السوق وكيفية إستخدامها في سياق التواصل مع المواطنين ومعرفة أية أداة إلكترونية تكون مفيدة أكثر في الظروف والضرورات الإجتماعية المختلفة. وبالرغم من تناولنا للأدوات في هذا الكتاب إلا أن ذلك لا يعني أن تلك الأدوات ثابتة ومستقرة بل كما تعودنا في عالم الإنترنت والتكنولوجيا فإن الثابت الوحيد هو عملية التغير الدائمة، ولكن إطار العمل الإلكتروني الإجتماعي قد بدأ يصل إلى مرحلة إستقرار نوعاً ما وهو ما تتشارك فيه جميع تلك الأدوات الإلكترونية الحالية والمستقبلية على الأرجح في المدى المنظور.

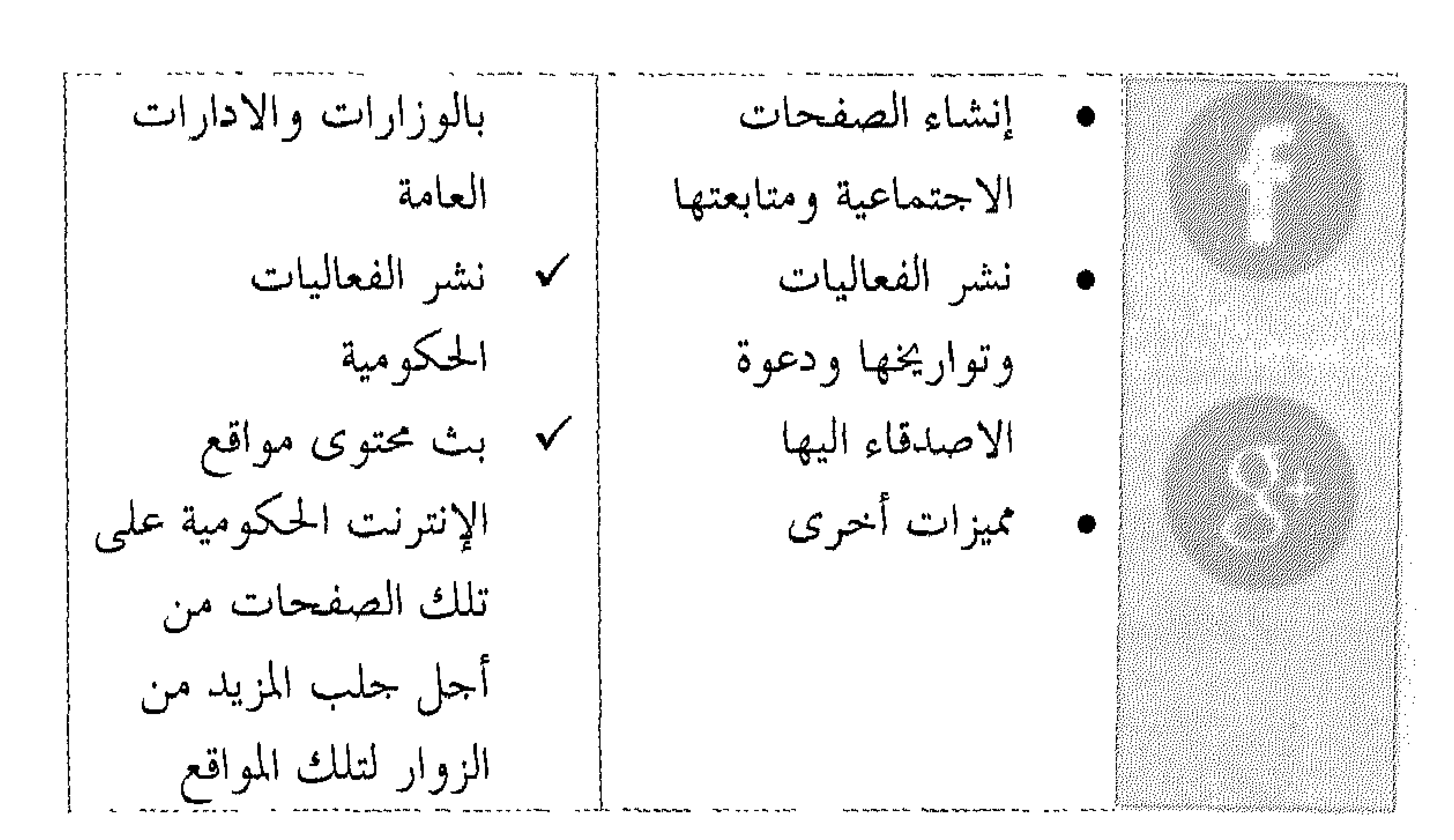
وبغض النظر عن الأداة أو المنصة سواء كانت فايسبوك أو تويتر أو غوغل بلاس أو أية أداة مستقبلية، سوف يستبطن إطار العمل الإجتماعي الإلكتروني في داخله المميزات التالية:

- القدرة على تكوين الصداقات الإفتراضية.
- إمكانية الإنخراط في المجموعات المتخصصة او التي يتم إنشاؤها لأسباب سياسية أو إجتماعية أو إقتصادية وغيرها.
- إمكانية متابعة الأفراد أو المجموعات أو المؤسسات أو الحكومات (Followers) من أجل البقاء على إطلاع على آخر أخبارهم ومستجداهم.
- ميزة مشاركة المواد المنشورة من فيديو وصور ونصوص بطريقة فيروسية (من شخص إلى آخر، إلخ...)
- محرّك تقديم الأصدقاء المحتملين (Recommendation Engine) وقد يكون هذا القسم من الشبكات الإجتماعية

قد ساهم بدور كبير في تطورها. ويعمل هذا المحرّك على إيجاد العلاقات المحتملة عبر مقارنة سلوكيات المستخدم وأصدقائه وإهتماماته مع مجموعة بروفيلات الأشخاص في نفس الدوائر من أجل تقديم الأشخاص الذين تنطبق عليهم بعض الشروط على أهم أصدقاء محتملين مما يعزز قيمة الشبكة الإجتماعية بشكل عام ويعزّز مشاركة ذلك المستخدم بطريقة أفضل.

- ميزة التواصل الخاص بين أفراد الشبكة الإجتماعية وقد أدخلت معظم المنصات الحديثة ميزة الدردشة المباشرة (Online Chat).
- إمكانية وسم المواد المنشورة بوسوم مكانية وعلى سبيل المثال مكان الصورة الجغرافي (Geo-Location)
- إمكانية التعامل مع المنصات الإلكترونية الإجتماعية من خلال واجهة الوب البرمجية بالإضافة إلى إمكانية بناء تطبيقات حكومية أو مؤسساتية تستفيد من البنية التحتية لتلك المنصات ومنها: تسجيل الدخول عبر تلك المنصات، إستخدام معلومات المستخدمين في عملية التسجيل في المواقع، النشر مباشرة من خلال برامج ومواقع خارجية على تلك المنصات.

الأدوات الإجتماعية الإلكترونية		
الأداة	الإستخدام	المغزى الحكومي (مثال)
يوتيوب	• مشاركة مقاطع الفيديو • إنشاء قناة إفتراضية	✓ نشر فيديو الإنجازات والمشاريع الحكومية ✓ نشر محاضر من جلسات البرلمان العامة ✓ نشر فيديو توعوي وتثقيفي ✓ نشر فيديو ترويجي وسياحي عن البلد
التويتر	• التدوين والأخبار السريعة (التغريد) • متابعة حساب المستخدمين (شخصيات، مؤسسات، حكومات، ...) واستقبال تغريداتهم	✓ تغريدات بشأن حالات الطوارئ ✓ تغريدات الأخبار والنشاطات والفعاليات في المدينة ✓ تغريدات إعلان الوظائف العامة
بنترست	• نشر الصور والأعمال الفوتوغرافية • إنشاء معارض فوتوغرافية ومشاركتها مع إمكانية متابعة تحديثاتها من قبل المستخدمين	✓ صور سياحية ✓ لوحات وبوسترات تثقيفية ✓ صور نشاطات الحكومة
فايسبوك وغوغل بلاس	• الشبكات الاجتماعية المتكاملة التي تسمح بتكوين الاصدقاء والمجموعات	✓ إنشاء صفحات حكومية للخدمات العامة ✓ صفحات خاصة



	• إنشاء الصفحات الاجتماعية ومتابعتها • نشر الفعاليات وتواريخها ودعوة الاصدقاء اليها • مميزات أخرى	بالوزارات والادارات العامة ✓ نشر الفعاليات الحكومية ✓ بث محتوى مواقع الإنترنت الحكومية على تلك الصفحات من أجل جلب المزيد من الزوار لتلك المواقع

جدول 5: الأدوات والمنصات الإجتماعية الإلكترونية

وكما ذكرنا سابقاً فإن الأدوات الإلكترونية الإجتماعية الموجودة حالياً في السوق ليس بالضرورة أن تستمر إلى ما لا نهاية، فقد يأتي يوم وينتهي الفايسبوك كما حصل مع ماي سبايس (MySpace) من قبله، ولكن المميزات التي ذكرناها أعلاه سوف تستمر بالظهور في أية منصة إجتماعية مستقبلية وهذا ما ينبغي للحكومات أن تتدرب عليه وتتجهز له وترسم إستراتيجياتها حوله من أجل البقاء في دائرة المشاركة والثقة مع المواطن.

الأمن الذكي في الحكومة

"نعمتان مجهولتان: الصحة والأمان"

حديث شريف

لماذا قطاع الأمن؟

قد يتساءل البعض لماذا اخترنا التوسّع في قطاع الأمن بالتحديد وشرح كيفية تطويره في سياق بناء مكوّنات الحكومة الذكية مع أن الحكومة تمارس نشاطها في مختلف القطاعات الإجتماعية، والإجابة على هذه التساؤلات بسيطة جداً حيث أن الأمن والإستقرار في أي بلد هما عماد الإرتكاز الأساسي في عملية تنمية الإقتصاد وإزدهار المجتمع، ومن دون أمن ذكي، قادر على "التنبؤ" بالمخاطر ونزع فتيلها قبل حدوثها أو الإستجابة السريعة للتهديدات الخطيرة التي تتعرض لها الدولة، فلن يشعر المواطن بالأمان وكذلك المستثمر الأجنبي أو المحلي.

وعملية إضفاء نوع من الذكاء على الممارسات الأمنية لأية حكومة قد أصبحت من الضرورات نظراً لتواجد الكثير من مكوّنات المجتمع في العالم الإفتراضي مع ما يعني ذلك من إنتشار غير مسبوق للداتا الشخصية والصحية والأمنية والمالية على الشبكات الإفتراضية والإجتماعية وإزدياد معدلات تعرضهم للخداع أو الإستغلال من المافيا او جهات خارجية عدوة أو من عالم إجرام الإنترنت على إختلافه. وفي

الجهة المقابلة، يتكاثر أعداء الدولة ايضاً على تلك الشبكات وهم يشعرون بحرية الإنتقال من حدود الدولة الإفتراضية إلى مقراهم الإستخبارية والإجرامية ببساطة لأنه لا يوجد حدود ونقاط تفتيش على الإنترنت.

وتواجه الدولة والحكومة أيضاً مخاطر تعرّض شبكاها وأنظمتها للهجوم الإلكتروني والتشويش والتخريب وعليها أن تكون جاهزة للدفاع عن وجودها الإفتراضي لأن ذلك يمس مباشرة مستقبل أجيالها وثقافتها ونظامها المالي والثقة فيه ونظامها الأمني والإعتماد عليه.

لقد تم بناء أجهزة الأمن في الدولة لكي تتعامل مع تهديدات واقعية ملموسة ولها آثار مشهودة، بينما يجري الطلب منها اليوم أن تتعامل مع تهديدات من نوع آخر: تهديدات لم يكن لها وجود منذ عقد من الزمن ولم تكن تلك الأجهزة مدربة ومجهّزة للتعامل مع ذلك النوع من المخاطر. والحكمة تقتضي أن تعيد أجهزة الأمن في البلدان العربية النظر في إجراءاها وتطويرها وهندستها بما يتناسب مع العالم الذكي، إن الأمن في العالم العربي بحاجة إلى أن يكون أمناً ذكياً يحافظ على مصالح المواطن الإفتراضية كما يحافظ على مصالحه المادية ويحمي الدولة من عمليات التجسس الرقمي واسعة النطاق التي تنتشر مؤخراً مثل انتشار النار في الهشيم.

الأمن المعلوماتي الحكومي

إن الأمن المعلوماتي يتم قياسه بمستوى صلابة وقوة أضعف نقطة فيه وليس أقواها، وقد بدأت الدول على إختلافها بإستغلال نقاط الضعف الأمنية الالكترونية التي نعاني منها كأجهزة وشعوب عربية وإسلامية وإنتقلت من مرحلة التجسس التقليدية التي انتشرت وسائلها

خلال الحرب الباردة إلى مرحلة التجسس الواسع النطاق والتي تعتمد على تجميع أكبر حجم من الداتا ومن مصادر مختلفة من أجل التنقيب عن الحقائق الأمنية والاستخبارية فيها. لم يعد الفرد آمناً معلوماتياً بسهولة لأن أمن الأفراد مرتبط بأمن المجموعات التي ينتمون إليها وأمن المجموعات مرتبط بأمن علاقاتهم الشخصية والعائلية وقد تؤدي معلومة واحدة من داخل هذه الحلقة إلى إنكشاف الحلقة بأكملها.

هذا وما تزال الفجوة تتسع كل يوم بين الذين يقومون ببناء ترسانات الأسلحة الرقمية وبين الذين يحاولون اللحاق بهم تماماً كما حصل في سباقات التسلح السابقة حيث كان العرب والمسلمون في أغلب الأحيان مستهلكين للسلاح و لم يكونوا يوماً منتجين له (إلا ما ندر)، وربما يشكل السلاح الرقمي اليوم تهديداً أكبر حيث أنه في الوقت الذي تشتريه الحكومات العربية للتجسس على أعدائها تكون الشركات المنتجة لهذه الأدوات المعلوماتية تتجسس عليها. إن السلاح الرقمي من الممكن إطلاقه في إتجاهين أو ثلاثة أو أكثر ويستعمل لمرات عديدة، بينما السلاح التقليدي له وجهة واحدة إما على الصديق أو على العدو وينتهي.

ويتوزع نشاط الأمن المعلوماتي على عدة مجالات ومنها ما يتعلق بالأمن الوقائي الإلكتروني ومكافحة التجسس الرقمي وإجراءات وأدوات كشف العملاء وتحركاتهم وصولاً إلى الأمن المادي لمراكز الدولة المعلوماتية والاستحواذ على مهارات وأدوات البحث الجنائي الإلكتروني والأمن المادي وأمن الأفراد وأمن الشبكات والإتصالات وفريق التدخل المعلوماتي وغيرها.

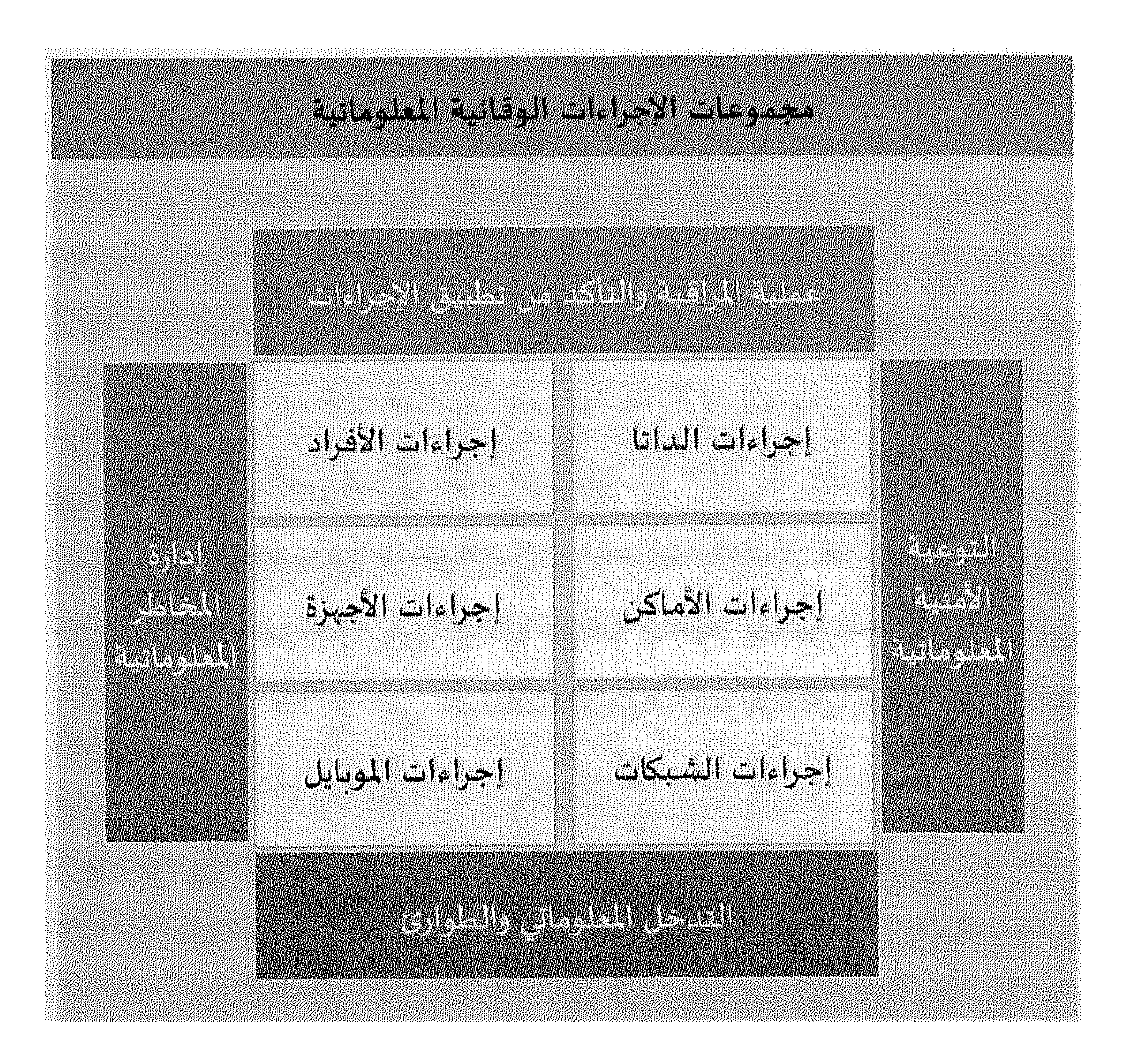
ونستطيع تفصيل بعض تلك المجالات على أن تختار الحكومات العربية كيفية إنشاء هيكليات تنظيمية تعتني بوظائف الأمن المعلوماتي إو إلحاقها بالدوائر الأمنية المتخصصة في الدولة:

الأمن الوقائي المعلوماتي

وهو أمن دفاعي بشكل عام حيث تعمل وحـــدات خاصـــة في الدولة على تأمين موارد المعلومات الحكوميـــة والعســـكرية والأمنيـــة والتأكد من عدم وقوعها تحت الأيدي الخطأ وتقوم في الوقت الـــنفس بتطوير الإجراءات والسياسات الأمنية المعلوماتية المناسبة ونشرها علـــى دوائر الدولة من أجل تطبيقها ومن تلك الإجراءات:

1. إجراءات نقل الداتا الحكومية من مكان إلى مكان مع التأكد من سلامتها خلال الطريق أو عبر الأســـلاك والشـــبكات، كذلك إجراءات الحفاظ على داتـــا الحكومـــة وأرشـــفتها وصيانتها وكيفية تلفها عند الضرورة.
2. إجراءات إعطاء صلاحية الدخول للداتا الحكومية الحساسة
3. إجراءات المتعاقدين مع الحكومة في مجال أمن المعلومات
4. الإجراءات الحمائية المتخذة في مراكز الداتا الحكومية
5. مستوى تشفير الداتا في حال الضرورة
6. إجراءات إستخدام الأجهزة الجوالـــة ووســـائط التخـــزين المحمولـــة (USB & BYOD Policies) داخـــل مراكـــز الحكومة
7. إجراءات التأكد من سلامة أجهزة المســـؤولين والأجهـــزة الحساسة من البرامج الملوّثة.

ويلخص لنا النموذج التالي المجموعات الإجرائية الرئيسية في الأمن الوقائي (طبعاً من دون تفصيل كل مجموعة إجرائية)



رسم توضيحي 12: سلة الإجراءات المعلوماتية الأمنية في الحكومة

وكما نعلم فقد أدى الخلل في الأمن الوقائي المعلوماتي التابع لوكالة الأمن القومي الأميركية في العام 2013 إلى أكبر عملية تسريب لوثائق كانت مصنّفة سرية من خلال المتعاقد إدوارد سنودن.

وبعكس ما يعتقد الكثير من الناس، فإن مشكلة الأمن المعلوماتي لا تكمن في أغلب الأحيان في الأنظمة البرمجية والأجهزة والخوادم خاصة عندما يكون هناك سياسات تنظيمية واضحة حول كيفية تركيب الأجهزة وتحديد مصادرها وتجهيزها وبرمجتها من قبل الخبراء، بل يكون البشر هم نقطة الضعف الأكثر تعرضاً للإختراق في المنظومة الأمنية.

وهذا بالتحديد ما حدث مع إدوارد سنودن ووكالة الأمن القومي الأميركي حيث كان السيد سنودن متعاقداً مع تلك الوكالة ويعمل معها في مجال إدارة بعض الخوادم والأنظمة وفي خلال أكثر من عام تمكن من تحميل ما يقارب 200 الف وثيقة من أنظمة وأجهزة تلك الوكالة.

ويكمن الخلل هنا في عدة مواطن:

1. **ضعف ولاء الموظف:** وهذه المشكلة لا يمكن كشفها بسهولة إلا من خلال دراسة عميقة نفسية للموظف المخول بالاطلاع على البيانات الأمنية السرية والبيئة التي يأتي منها والعقائد التي يعتقد بها وغيرها.
2. **انت من الداخل إذن انت آمن:** لقد كشفت إختراقات سنودن ضعفاً في إدارة المعلومات في وكالة الأمن القومي الاميركي ومنها كيف يتم السماح لموظف بالإطلاع على هذا الكم الهائل من البيانات من دون أن يكون هناك تحديد صلاحيات الدخول إلى المعلومة حسب طبيعتها وسريتها وليس حسب الشخص الذي يطلع عليها.
3. **وهن نموذج كلمات السر:** يعاني عالم أمن المعلومات اليوم من مشكلة "كلمة السر" حيث أن تلك التقنية لم تعد آمنة للحفاظ على المعلومات وبالتالي بدأت المنظمات بالإتجاه إلى تقنيات أكثر أمناً منها، وقد كشفت المعلومات ايضاً أن السيد سنودن حصل على كلمات السر من عشرات الموظفين بعد أن أقنعهم بأنه يعالج بعض المشاكل الفنية وهو بحاجة إلى كلمات المرور منهم مما خوّله من الاطلاع على مزيد من المعلومات من خلال أجهزة وأنظمة أولئك

الأشخاص، وهنا يظهر أحد مكامن الخلل الإضافية في إدارة وكالة الأمن القومي الاميركي وهو عدم إتباع إجراءات واضحة أو وجود سلسلة من المسؤوليات والتراخيص قبل الولوج إلى مصادر الداتا الأساسية.

وبالعودة إلى موضوع الإجراءات والسياسات فنحن نسأل هل كان بالإمكان لتلك الوكالة أن تتفادى ذلك الاختراق الأمني الداخلي لو اتبعت سياسات وإجراءات معلوماتية واضحة؟ والجواب هو كان من الممكن إلى حد كبير تفادي ذلك الاختراق لو كانت الإجراءات الأمنية الإلكترونية التالية محترمة وقيد التنفيذ:

- **سياسة وإجراءات الأجهزة المحمولة**: تبين أن إداورد سنودن قد قام بتهريب معظم تلك الوثائق على "USB فلاش" وهنا نسأل كيف تم السماح لموظف معين بإدخال جهاز التخزين المحمول هذا الى وكالة أمنية بذلك الحجم؟
- **سياسة وإجراءات الدخول إلى الداتا**: كيف يتم السماح لموظف بالحصول على حق الدخول لأجهزة وأنظمة خارج نطاق اختصاصه حتى ولو كان يعمل في مجال الدعم والصيانة من دون العودة إلى سلسلة إجرائية إدارية تفهم وتوافق على رفع مستوى حق الدخول لذلك الموظف وتحديد متى ينتهي ذلك الحق ومن يأخذه منه وكيف يتم التأكد من ذلك؟

نظراً إلى حجمها والأموال التي تنفق عليها فقد أخفقت وكالة الأمن القومي الأميركي إخفاقاً كبيراً في موضوع تسريب معلوماتها وإستراتيجيتها الأمنية الإلكترونية حيث كانت الوثائق والداتا تمر من تحت أقدامهم وهم غير واعين لما يحصل. وللعلم فإن وكالة الأمن

القومي من مهمتها حماية معلومات الدولة والمعلومات الأمنية من الإختراق فإذا بها تفشل في حماية معلوماتها والسبب ليس خطأ تقني إنما خلل بشري!

البحث الجنائي الإلكتروني

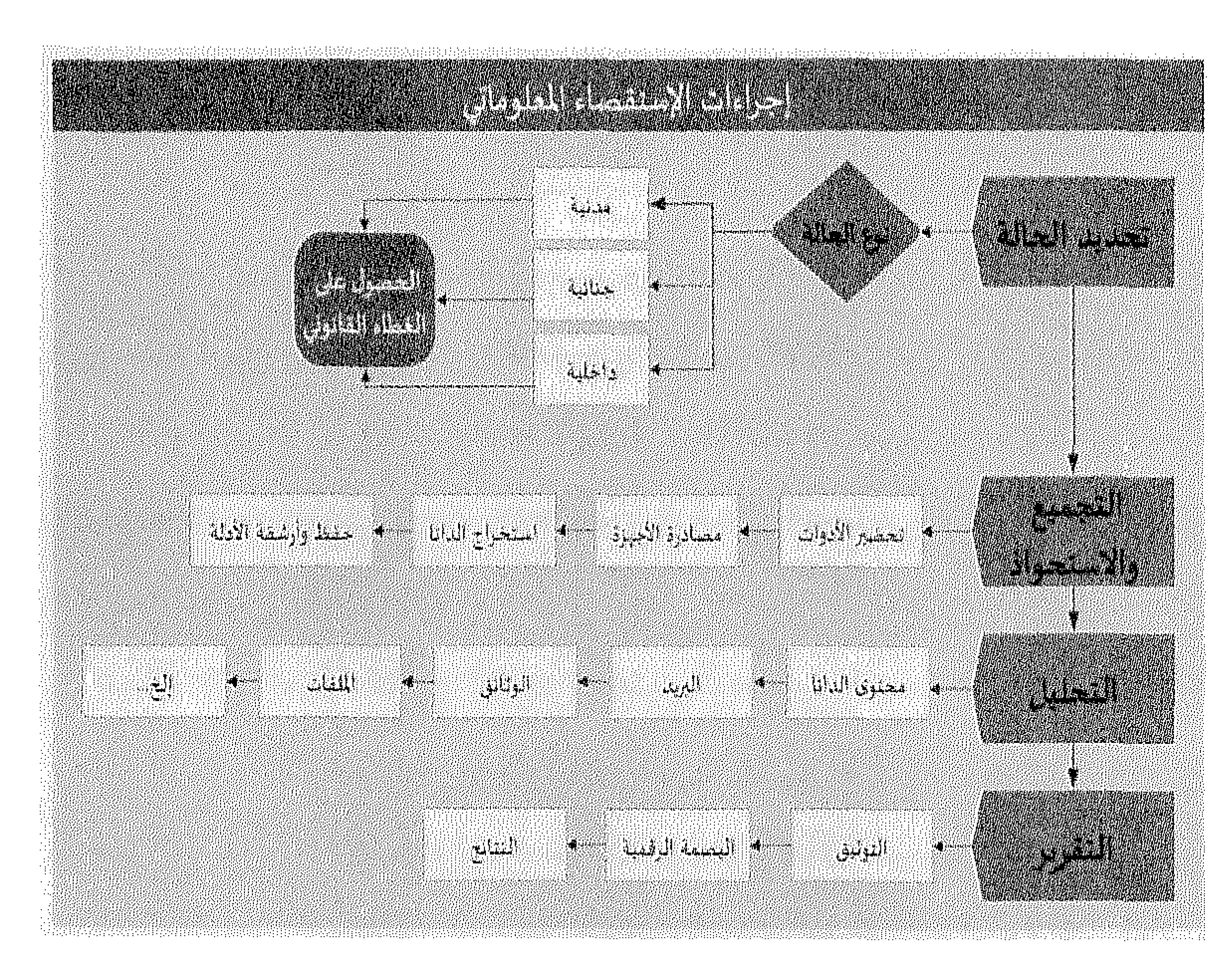
وهو فرع من فروع الأبحاث الجنائية يعتني بالتنقيب عن داتا وآثار إلكترونية تساعد على كشف الجرائم أو المتعاونين فيها وملاحقة الأهداف التي تحددها الدولة على أنها أهداف عدوة بشكل عام. وكما المواطن الذي وجد في الإنترنت والهواتف والشبكات وسيلة راحة ورفاهية وسهولة كذلك عالم الإجرام والمافيا والعملاء وجدوا في تلك الوسائل والأدوات مرتعاً خصباً لسرقة الأموال أو التجسس والإبتزاز وإدارة الأنشطة الغير مشروعة، وهم بالتالي يتركون آثاراً في ساحة الجريمة الإفتراضية عن عمد من أجل التضليل أو عن جهل أو عن طريق الخطأ. وهنا بالذات يمكن للأمن في الدولة التدخل من إجل إيجاد كل تلك الآثار الرقمية والخيوط وربطها ببعضها البعض من أجل إنتاج حقائق أمنية تساعد في عملية الكشف الأمني والمخابراتي عن الأعداء.

والمجالات التي يهتم بهم الاستقصاء الإلكتروني واسعة نذكر منها: التحرش والابتزاز الجنسي، تجارة البشر، تجارة الممنوعات بشكل عام على الإنترنت، سرقة بطاقات الإئتمان، سرقة هوية الأشخاص وحساباتهم الالكترونية، الترويج للعدو أو التعاون الالكتروني معه.

ويعتني البحث الجنائي الإلكتروني بجميع أشكال وأنواع الداتا المتوفرة في الأجهزة التي تم مصادرتها من مسرح الجريمة سواءٍ كانت موجودة في أجهزة الكمبيوتر أو أجهزة الهاتف الذكي أو كاميرات

المراقبة الرقمية ووسائط التخزين المحمولة حيث تساهم آليـــات وأدوات إستعادة الداتا بعد حذفها في هذا العمل. وقد طرح العديد من خـــبراء الأمن المعلوماتي منهجيات عملية لمقاربة موضوع الإستقصاء المعلوماتي نذكر منها منهجية الخطوات الستة للسيد كاسي (2001) والتي تعتمد الخطوات العامة التالية:

1. تحديد وتقييم الحالة الأمنية المعلوماتية
2. تجميع الأدلة الرقمية والاستحواذ على الأجهزة
3. حفظ الأدلة الرقمية وأرشفتها
4. معاينة الأدلة الرقمية
5. تحليل الأدلة الرقمية
6. إعداد التقارير ونتائج البحث



رسم توضيحي 13: نموذج كاسي المعدّل لإجراءات الإستقصاء المعلوماتي

ومن دون أدنى شك، فإن الأبحاث الجنائية الإلكترونية هو مجال واسع يتطرق إلى أدوات إستخراج المعلومات من الداتا التي يتم الاستحواذ عليها وكيفية إستخدام تلك الأدوات والتأكد من عدم العبث "بالمسرح الإفتراضي" للجريمة أو الأدلة الرقمية وهو خارج نطاق هذا الكتاب.

التجسس الرقمي في الحكومة

في الوقت الذي تمارس أجهزة الحكومة مهمة الأمن الوقائي المعلوماتي تقوم كذلك بممارسة النشاط الإستخباري والتجسسي المعلوماتي من أجل تجنب المخاطر والتهديدات قبل حدوثها. وعادةً ما تنشر أجهزة الأمن المختصة في الدولة ترسانتها التجسسية الرقمية عبر تركيب أجهزة خاصة عند مزودي خدمات الإنترنت ومقاهي الإنترنت العامة او عبر البرامج المختلفة وتطبيقات الجوال وشبكات التنصت والكاميرات الرقمية في الأماكن العامة ومواطن الخطر والتهديد.

وعادةً ما تحتاج عمليات التجسس الرقمي إلى غطاء قانوني وتشريعي حتى لا يتم إساءة إستخدامه وتجييره لمصالح خاصة أو فردية أو توظيفه في الإستغلال السياسي. وينقسم التجسس الرقمي مخابراتياً إلى عدة مستويات ومنها: التجسس الرقمي الوطني من أجل مكافحة الجريمة والشبكات الإرهابية وكشف العلاقات بين أفراد تلك المجموعات وكذلك يوجد التجسس الرقمي الصناعي والتجاري حيث مارسته بعض الحكومات سراً من أجل تحصيل الأفضلية في ميدان الأعمال عبر سرقة نماذج الإختراعات والتصاميم المهمة والوثائق السرية وهذا ما تم الكشف عنه في الوثائق المهرّبة من وكالة الأمن القومي الأميركي عبر المتعاقد إدوارد سنودن. ويبقى مجال حيوي آخر وهو مجال مكافحة التجسس الرقمي الذي تقوم به الدول ووكالات المخابرات العالمية والمنظمات الإرهابية ضد الدولة.

نبذة من أدوات التجسس الرقمي		
شبكات بوتنت (Botnet)	نشر فيروسات تجسسية تقوم بسرقة الوثائق والصور والمكالمات وإرسالها إلى خادم القيادة والسيطرة. مثال الفيروس فليم وغوس وزيوس.	إستراتيجي محلي — خارجي
كاميرات المراقبة الرقمية	مراقبة الأماكن العامة وتسجيل الحركة بصورة مستمرة.	إستراتيجي محلي
الفيروسات الموجّهة Targeted) (Malware	برامج ملوّثة تستهدف أشخاصاً معينين أو مؤسسات محددة (الفيروس شمعون الذي استهدف شركات نفط في الخليج)	تكتيكي محلي — خارجي
برامج ملوّثة	عادة ما تستخدم البرامج الملوثة من أجل تحميل فيروسات تجسس على أجهزة الضحية	تكتيكي
وسائط تخزين محمولة ملوّثة	يتم تحميل فيروسات تجسسية على شرائح (Poisoned USB) حيث تقوم بتحميل نفسها على أجهزة الكمبيوتر بمجرد إدخالها وفتحها	تكتيكي
أجهزة تنصت داتا مزودي الإنترنت	أجهزة خاصة يتم تركيبها عند مزودي الإنترنت من أجل تسجيل حركة المشتركين وجميع الداتا الصادرة والواردة منهم وإلى الإنترنت	إستراتيجي محلي - مشتركين

جدول 6: نبذة من أدوات التجسس الرقمي

يظهر لنا الجدول السابق بعض أنواع ادوات التجسس الرقمي والتي لا سبيل لحصرها نظراً لتطورها بشكل يومي، علماً أن عملية تطوير تلك الترسانات التجسسية تقوم بها الحكومات ومافيا الإنترنت وبعض المحترفين على حد سواء.

النظام الأمني المعلوماتي

إن رد الفعل الأمني الحكومي على التهديدات والمخاطر لا يمكن أن يكون فعّالاً من دون تكوين صورة كاملة وشاملة عن "الحالة" الأمنية أو الجنائية التي يتم التعامل معها. وعلى سبيل المثال، قد لا تفيد داتا الإتصالات لوحدها في تحديد الأهداف التي تراقبها أجهزة الأمن في الدولة وكذلك قد تستفيد تلك الأجهزة إلى حد قليل من عناوين بعض الأماكن المرتبطة بتلك الأهداف ولكن تجميع أجزاء تلك الوقائع والداتا وربطها مع بعضها والبعض وإستنباط حقائق أمنية جديدة ثم إضافة معلومات موجودة سابقاً إلى كل هذا الخليط المعلوماتي قد يؤدي إلى كشف أمني حقيقي ونزع فتيل التهديد المباشر لأمن الدولة أو أمن مواطنيها ومؤسساتها. ومع تضخم حجم الداتا المخابراتية والداتا الرقمية الناتجة عن أدوات التجسس المختلفة تصبح عملية التحليل والاستنتاج صعبة وطويلة ومعقّدة على ضباط الأمن الحكومي وهنا يأتي دور النظام الأمني المعلوماتي والذي يتم بناؤه وتطويره من أجل ضبط إيقاع هذه الحركة المعلوماتية الضخمة لدى أجهزة الأمن في الدولة. ويتكون النظام الأمني المعلوماتي من عدة أقسام كل منها متخصص في تجميع وتحليل نوع معين من الداتا.

ويبين لنا النموذج التالي صورة منطقية عن نظام معلوماتي أمني عام:



رسم توضيحي 14: النظام الأمني المعلوماتي في الحكومة

ويعمل النظام الأمني المعلوماتي بطريقة "خط الإنتاج" حيث تدخل الداتا الخام من مختلف المصادر التجسسية مثل داتا التطبيقات وداتا الشبكات الإجتماعية وكاميرات المراقبة الرقمية ومعلومات المخبرين عن الأرض وداتا أجهزة الإستشعار على إختلافها والمعلومات الصحية والمالية ووسائل النقل الخاصة بالأفراد ومعلومات المركبات والسيارات والأماكن والعناوين، تدخل هذه الداتا في طبقة العمل الأولى في النظام وهي وحدة "الاستقبال والفلترة والتوجيه" حيث يتم إستلام الداتا الرقمية وفحص أنواعها إلكترونياً ثم تحويل كل نوع إلى النظام الفرعي الخاص بمعالجته.

وتستلم الطبقة الثانية من النظام تلك الداتا حسب نوعها حيث يتم فرزها إلى الأنظمة الفرعية التالية:

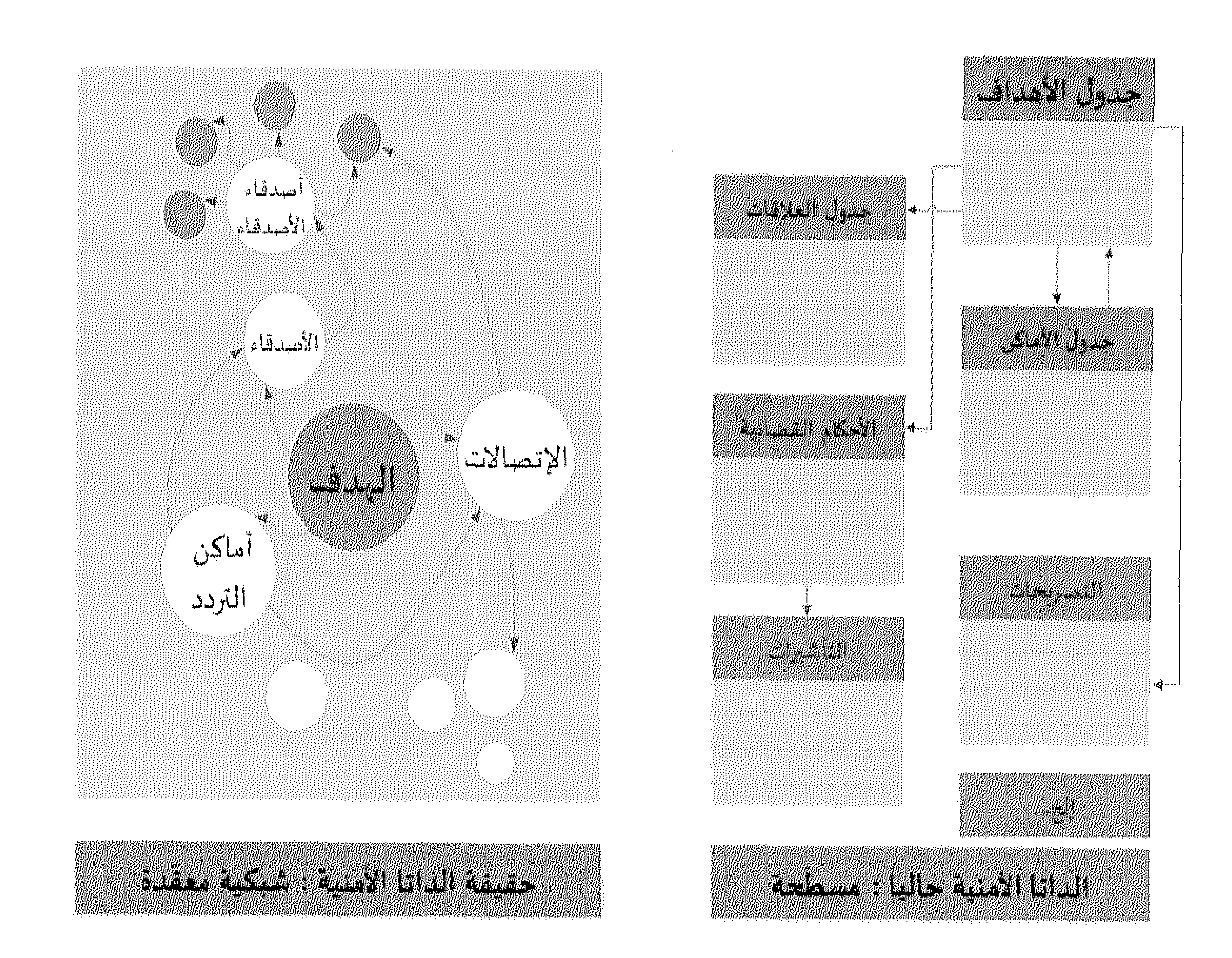
- **نظام معالجة الصور:** والذي يعمل على إستخراج الداتا الوصفية والداتا المكانية والزمانية (تاريخ وأوقات الصور) من تلك الصور مع إمكانية التعرف على الوجوه إذا توفّرت. ثم يجري تحويل النتيجة إلى قاعدة البيانات الشبكية الخاصة بالنظام بعد أن يتم ربط النتائج بالأفراد موضوع الحالة الأمنية.
- **نظام معالجة مقاطع الفيديو والصوت:** يعمل هذا النظام الفرعي ايضاً على إستخراج المعلومات المكانية والزمنية من تلك الداتا مع إمكانية تحليل الضجيج المرافق لتلك المقاطع من أجل تحديد طبيعة المكان الذي تم فيه أخذ التسجيلات وبالنهاية يتم ترحيل كل الداتا الناتجة إلى قاعدة البيانات المذكورة سابقاً.
- **نظام إستخراج الأسماء والمفردات:** مع تطور الآليات الرقمية في مجال تحليل اللغات البشرية أصبح بالإمكان التعرف على الأسماء او المفردات المهمة في الوثائق ورسائل البريد الالكتروني والملفات الخاصة، ويعمل هذا النظام الفرعي على الاستخراج الاتوماتيكي لتلك البيانات ثم ربطها بشبكة العلاقات التابعة للحالة الأمنية.
- **نظام إستخراج الداتا الوصفية من الوثائق:** تحمل معظم الوثائق الرقمية في داخلها بيانات عن المستخدم والوقت الزمني لكتابة تلك الوثائق والمعلومات الأخرى المهمة التي يتم إستخراجها اوتوماتيكياً عبر هذا النظام الفرعي وربطها بقاعدة بيانات النظام.

وعند الإنتهاء من عمليات المعالجة في الطبقة الثانية للنظام المعلوماتي تكون الأجهزة الحكومية قد حصلت على خليط مترابط من الأمكنة والعناوين والتواريخ والأزمنة مدعومة بصور رقمية ووسائط ميديا مع إمكانية البحث فيها وكشف العلاقات بينها وبين داتا موجودة سابقاً عند تلك الأجهزة.

وبالطبع فإن مسؤولية إدارة النظام سوف تقع على وحدة مركزية في أجهزة الدولة حيث تمنح صلاحيات الدخول والإدخال للأفراد المعنيين حسب حاجاتهم وتتحمل مسؤولية سلامة النظام والداتا الموجودة فيه وكافة الإجراءات المعنية بحمايته.

التمثيل الصحيح للداتا الأمنية

لقد إستخدمت أجهزة الدولة الأمنية التكنولوجيا المتوفرة في السوق من أجل تمثيل الداتا وحفظها ثم إستخراجها لاحقاً، وتعتمد معظم قواعد بيانات الحكومة اليوم على أنماط الداتا الجدولية العلائقية (Relational Data) وهذا التمثيل للداتا الإستخبارية الحكومية يفترض أن تكون تلك المعلومات "مسطّحة" مثل أن يتم بناء قاعدة بيانات المجرمين من خلال مجموعة من الجداول تبدأ بجدول معلومات المجرم ويرتبط به مجموعة جداول معلوماتية منها على سبيل المثال ولا الحصر: جدول السيارات، جدول الأماكن، جدول الهواتف، إلخ...بينما نعلم أن واقع الداتا الأمنية والاستخبارية هو أنها داتا "شبكية معقّدة" مثل أن يرتبط شخص بمجموعة من الأفراد الذين يرتبطون بمجموعة أخرى وتلك ترتبط بأماكن وعناوين ومنها تصدر إتصالات هاتفية ومجموعة صور فوتوغرافية وإلى ما هنالك من تعقيدات تنتج عن الحركة الطبيعية لعالم الإجرام أو تنتج بطريقة تسميم الداتا من أولئك من أجل تضليل التحقيق الجنائي.



رسم توضيحي 15: نقل الداتا الأمنية إلى التمثيل الصحيح

وبناءً على ما تقدم، فإنه يصبح من الضروري لأي أمن حكومي ذكي أن يتعامل مع الداتا الإستخبارية والأمنية حسب طبيعتها الأصلية ومحاولة تمثيلها داخل مخازن الداتا بتلك الطبيعة أي شبكية قادرة على التوسّع وإضافة وسوم تعريفية على أي كيان معلوماتي (فرد، مؤسسة، تنظيم، إلخ...) يقع ضمن دائرة الإستهداف الأمني الحكومي.

الحكومة والحرب الإلكترونية

"الاستراتيجية من دون تكتيك هي اطـول الطـرق للنصـر والتكتيك من دون إستراتيجية هو الضجيج قبل الهزيمة"

الجنرال صن تزو

ظهور الذراع الرابعة

عادةً ما تتشكل الجيوش الحربية الحديثة من ثلاثة أذرع عسـكرية وهي القوة الجوية والقوة البرية والقوة البحرية تستخدمها للهجوم على أعدائها والدفاع عن أرضها. ولكن في عصر الإنترنـت والاتصـالات بدأنا نسمع عن معارك يدور رحاها في الفضاء الالكتروني وبين خصوم معظهم مجهول الهوية يهاجمون البنية التحتية الرقمية للدول التي يصنفونها في خانة العدو حيث تهدف الهجمات الرقميـة الى الحصـول علـى معلومات مخابراتية حساسة أو تدمير بنية الاقتصاد الذي بدأ يعتمد على المعلومات بشكل كبير أو لمجرد إشعار العدو أنهم موجودون على الجبهة الرقمية وبإمكانهم إزعاجه.

الصين وروسيا والولايات المتحدة الاميركية والكثير من الـدول العربية والإقليمية وغيرهم من الدول بدأت بتشكيل خلايا غير معلنـة ضمن تشكيلاتها الأمنية والعسكرية مهمتها القيام بهجومات الكترونيـة على نطاق واسع ضد أعدائها ومؤازرة أي حرب حقيقية قد تقع عـبر

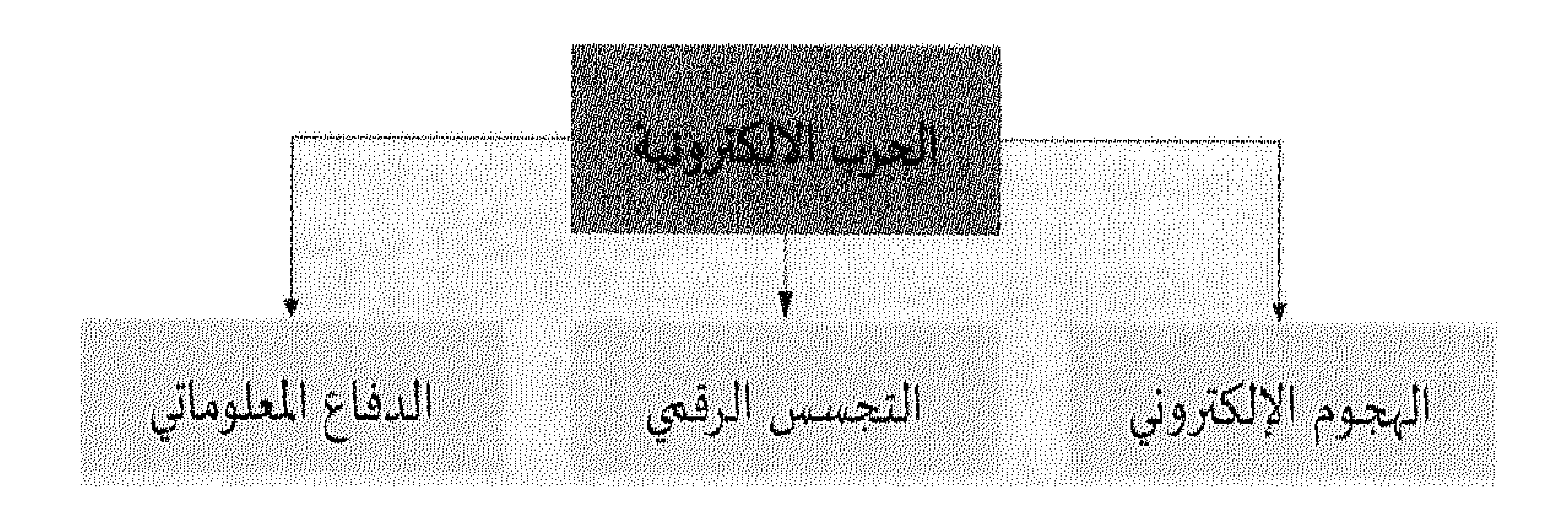
توظيف المعلومات والاتصالات إلى أقصى حد. لقد ظهــرت الــذراع الرابعة للجيوش العسكرية وهي القوة الإلكترونية والمعلوماتية ولكنها ما زالت خفية وغير معلنة كطبيعة الميدان الرقمي الافتراضي الذي تعمــل فيه.

وكما تحدثنا عن تشــكيلات وأدوات الأمــن المعلومــاتي في الحكومة الذكية، لا بد من الحديث عن قدراتها الهجومية والتجسسية الواسعة النطاق في العالم الإفتراضي، وعن إمكانية الردع الرقمــي وقواعد الإشتباك الإلكترونية حتى تكون تلك الحكومة قادرة علــى الدفاع عن منظوماتها الذكية بعد أن إستثمرت فيها الكثير من الموارد البشرية والمادية، حيث لا تكفي تشكيلات الجــيش الكلاســيكي لحماية موارد حكومية غير كلاسيكية من التخريب أو التلاعــب أو زعزعة الثقة.

ما هي الحرب الإلكترونية

لم نسمع حتى اليوم تعريفاً موحداً للحرب الالكترونية حيث أن معظم الإشتباكات الالكترونية هذه الأيام تتم من قبل منظمات وأفراد بغية الحصول على المال أو الانتصار لعقيدة معينة أو الانتقــام مــن منافسين و لم تتطور حتى اليوم تلك الحرب لكي تصل إلى أن تكــون جزءاً من حرب علنية تجري بين دولتين بالرغم من بــدايات ظهــور مؤشرات عليها في حربــي روسيا-استونيا وروسيا-جورجيا حيــث تزامن الهجوم الالكتروني بطريقة منظمة على البنية التحتية للمعلومات في جورجيا واستونيا مع العمليات العسكرية التي كانت تدور علــى الارض، وبالرغم من أن روسيا لم تعلن صراحة انها قامــت بتلــك الهجومات الالكترونية إلا أن التقارير على الإنترنــت تشــير إلى أن

مجموعات المهاجمين الالكترونيين الروس مرتبطة بطريقة أو بـأخرى بمنظومة السلطة والسيطرة الروسية وتتلقى تعليماتها وتوجيهاتها منها. وتمثل الحرب الالكترونية مخاطر جمة على الدول النامية التي أرادت من ناحية توطين التكنولوجيا وإحراز التقدم في المجال التقني ومن ناحية أخرى لم تتقدم في مجال الأمن المعلوماتي والالكتروني حيث بقي التفوق في هذا المجال بيد الدول الكبرى والدول المصنعة لبرامج المعلوماتية. ويجري اليوم سباق نحو التسلح الرقمي بين الدول وعلى رأسها أمريكا والكيان الصهيوني وكوريا الشمالية والصين وايران وروسيا من أجل توظيف تلك الإمكانيات في أي حرب عسكرية قادمة. وللعلم فإننا نركز في هذا الكتاب على الحرب الالكترونية المعلوماتية التي تعتمد بشكل كبير على البرامج والأنظمة والشبكات والإنترنت ولا نتطرق بالتفصيل إلى جميع قطاعات الحرب الالكترونية ومنها التشويش والرادارات وأجهزة التجسس والأدوات الكهرومغناطيسية وغيرها.



رسم توضيحي 16: اقسام الحرب الالكترونية

ومن الممكن أن نقوم بتقسيم الحرب الالكترونية إلى عدة مجالات أولها مجال الدفاع الالكتروني والذي يعنى بالدفاع عن انظمة وأجهزة ومعلومات الدولة والجيش والمخابرات والمجتمع وثانيها الهجوم الالكتروني وهو المجال الذي يتمثل بالعمليات الالكترونية التي تهدف الى التشويش على مصادر المعلومات وتدميرها وحرمان العدو من استخدامها لصالحه خلال اوقات الأزمات أو الحروب العسكرية والمجال الثالث هو مجال التجسس الرقمي وقد شهدنا منذ فترة اكتشاف شبكة الشبح الرقمية الصينية التي تجسست على أكثر من 100 دولة ومن دون أن يتم إكتشافها إلا مؤخراً.

ولكن يبقى السؤال الذي يتبادر الى الذهن هل يمكن للحرب الالكترونية وحدها أن تربح المعركة؟ والجواب هو ان النتيجة تعتمد على طبيعة المعركة الالكترونية:هل هي معركة إلكترونية سياسية تهدف الى تغيير الرأي العام بمعتقدات معينة او أحزاب؟ هل هي معركة إلكترونية ثقافية تهدف إلى إفراغ عقول الشباب من محتواها؟ أو معركة إلكترونية تجسسية ومخابراتية؟ الظاهر أن الأخيرة قد نجحت حتى الآن في أهدافها.

مخاطر الحرب الإلكترونية

قبل أن نتعمق في شرح مجالات الحرب الالكترونية من المهم أن نتعرف على مخاطر تلك الحرب وكيف يمكن أن تؤثر في مستقبل الحروب العسكرية أو العلاقات بين الدول، ومن أجل التمحيص أكثر يمكن الحديث عن الحرب الالكترونية البحتة التي تجري في الفضاءات الالكترونية للدول والمنظمات وتقتصر على تلك الفضاءات ومن دون إعلان كتلك التي تتم بنية الحصول على معلومات سرية وقد ذكرت

مجلة الوول ستريت في هذا المجال عن مسؤول سابق في الادارة الاميركية أن مخططات سرية للمقاتلة الشبح الجديدة F35 قد تمت سرقتها عبر زرع برامج تجسسية في أجهزة بعض الموظفين العاملين في الشـــركات التي تقوم بتنفيذ أجزاء من المشروع مثـــل شـــركتي BAE systems وLockheed Martin ولم تستطع إدارة المشروع من تحديد مـــا هـــي الملفات التي تمت سرقتها لأن البرامج التجسسية قامت بتشفير المعلومات قبل سرقتها وإرسالها الى قيادة تجسس إلكترونية في بلد معين وقـــد تم الحديث أن الصينيين ربما هم الذين فعلوها. والثانيـــة هـــي الحـــرب الالكترونية المؤازرة للعمليات الخاصة مثل محاولـــة تشـــويش رادارات كشف الطيران الحربـــي واختراقها قبل القيام بعملية أمنية عســـكرية محدودة والثالثة هي الحرب الالكترونية التي تتم بالتنسيق والارتباط مع الحرب العسكرية حيث يجري التجسس على الاشارات والاتصـــالات الصادرة عن أجهزة العدو مثل الهواتف النقالة وكـــاميرات الإرســـال المباشر واللاسلكي ومحاولة اختراق منظومة التحكم والسيطرة التابعـــة للعدو وصولاً إلى إمكانية التحكم بالاشارات الصادرة عـــن الاقمـــار الصناعية والتي تهدف الى توجيه الضربات الجوية والبحرية الصـــاروخية وغيرها. على صعيد آخر، قد يتم التصعيد في الحرب الالكترونية لكي تطال مصالح المدنيين والمؤسسات والاقتصـــاد في البلـــدان المتحاربـــة كالهجومات الالكترونية على أنظمة المصارف الالكترونية مـــن أجـــل ايقافها اذا لم يكن بالامكان اختراقها أو محاولة التخريب في شـــبكات الكهرباء العاملة بالتكنولوجيا الذكية (Smart Grid) وأنظمـــة الإدارة الصناعية وحتى شبكات الهواتف السلكية والجوالة.

وفي معظم الأحوال فإن الضربات الالكترونية التجسسية الموجعة والمؤلمة هي تلك التي تعتمد على العملاء المزروعين في الـــداخل مـــن

أجل فتح بوابات إلكترونية خلفية للعدو من أجل الولوج إلى معلومات وبيانات المواطنين مثل الذي حصل في لبنان حين اكتشفت الأجهزة الأمنية اللبنانية بطريقة ذكية كيف استطاع بعض الموظفين في أحد شركات الإتصالات الخلوية من تمكين العدو من التحكم ببعض مفاصل الشبكة الخلوية الخاصة بتلك الشركة. إن عدم اعتماد إطار متكامل للدفاع الاستراتيجي الالكتروني عن الوطن من الممكن أن يؤدي إلى اختراقات عديدة ومتتالية ومتعاظمة الخطر كلما ازداد اعتمادنا على الإنترنت وتكنولوجيا الاتصالات وهذا تماماً الذي يحصل اليوم.

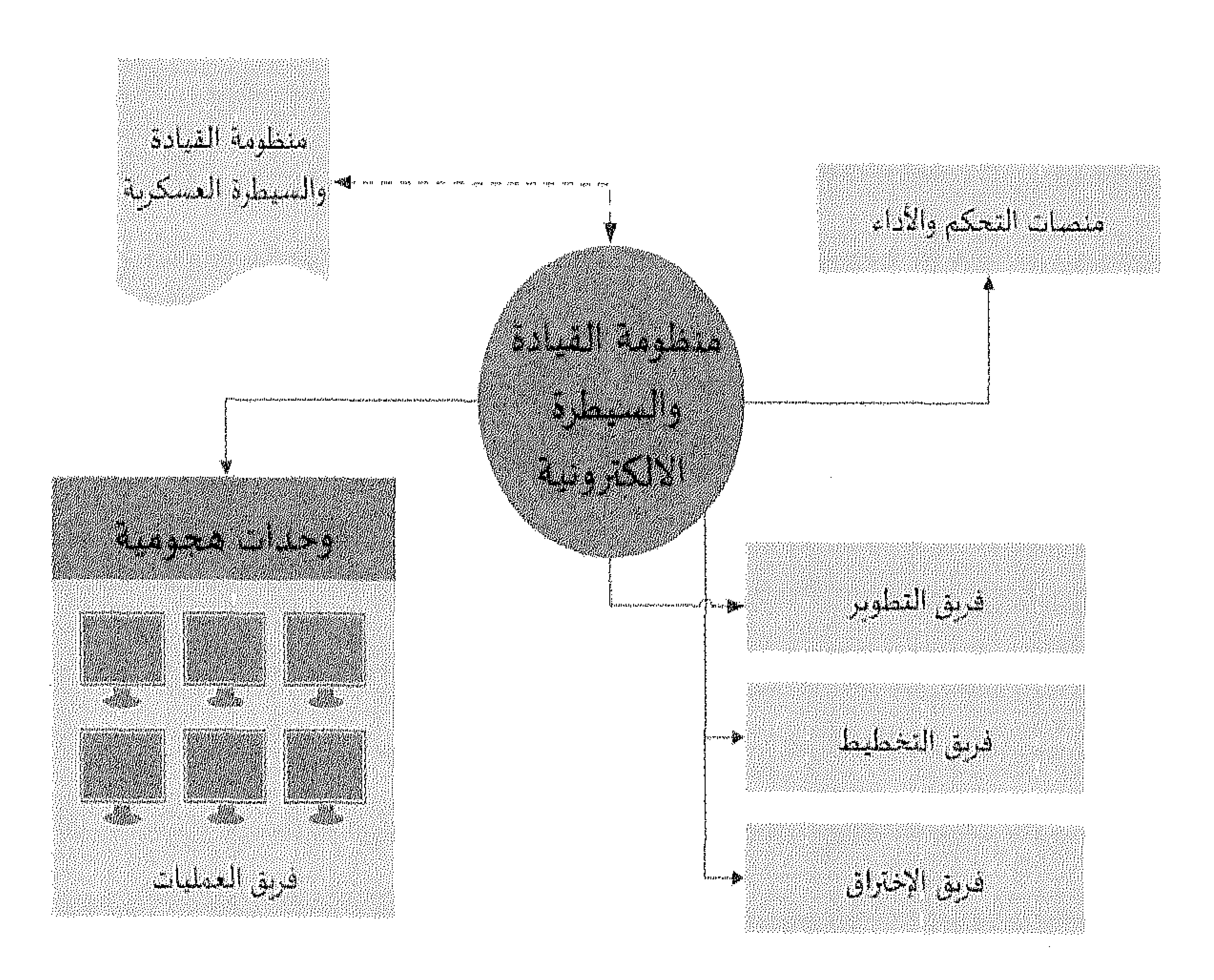
ومن مخاطر الحرب الالكترونية نستطيع أن نعدد أيضاً: إمكانية توقف الإنترنت كلياً في بلد معين، وبالتالي توقف البنوك على الإنترنت والمعاملات الالكترونية ومعاملات الحكومة الالكترونية والتطبيقات الذكية، أو سرقة أرقام وتفاصيل بطاقات الإعتماد التي يتم التسوق بها عبر الإنترنت أو تغيير النصوص الموجودة في بعض المواقع الحكومية اذا تم اختراقها مثل أن يتم الإعلان عن حالة طوارئ كاذبة على موقع وزارة الأمن الوطني بحيث تسبب الهلع العام. ومؤخراً بدأت بعض أجهزة المخابرات بالتلاعب بالأمكنة الجغرافية على خرائط غوغل الالكترونية من أجل تمويه بعض المعالم او إيهام العدو بوجود مراكز معينة متخصصة بأعمال عسكرية بينما هي مراكز مدنية.

منظومة القيادة والسيطرة

حتى تكون فعّالة تحتاج منظومة السلطة والسيطرة الالكترونية الى عدة عناصر مجتمعة وهي القيادة الالكترونية (وحدة التحكم) التي تحدد

الأهداف وتصدر الأوامر والوحدات الهجومية الالكترونية التي تقوم بتنفيذ تلك الأوامر وطريقة للإتصال والتواصل بين القيادة والوحدات الهجومية. وبما أن وحدة التحكم أو القيادة هي الجزء الأهم في تلك المنظومة نظراً للمسؤولية التي تقع على عاتقها بإطلاق إو إيقاف الهجوم الالكتروني وتقييم الأضرار والتأقلم مع التحديات الجديدة يجب أن تكون وحدة التحكم الالكتروني في منظومة السلطة والسيطرة محصنة ضد التدمير او الإختراق فإذا تم تدمير أجهزة الكمبيوتر التي تتحكم بالهجوم الالكتروني فإن الوحدات الهجومية المرتبطة بها سوف تبقى من دون رأس وبالتالي يتم إيقافها أو تصبح برامج ميتة لا تستجيب لأي أمر الكتروني تالي. ومن الممكن حماية وحدة التحكم الالكتروني بإعتماد أحد التقنيات التالية:

1. استنساخ وحدة التحكم الالكتروني وإبقاؤها جاهزة للعمل بشكل مباشر عند تدمير وحدة التحكم الأولى ويجب عدم تشغيل وحدات التحكم الالكترونية في نفس الوقت حتى لا يتم كشفها جميعاً بل ينبغي تشغيلها الواحدة تلو الأخرى
2. تحديث الوحدات الهجومية الالكترونية بعناوين وحدات التحكم بطريقة ديناميكية حتى تبقى على اتصال دائم بمنظومة السلطة والسيطرة.
3. تشفير المعلومات الصادرة من وحدة التحكم الى الوحدات الهجومية الالكترونية وبالعكس حتى لا يتم اعتراض المعلومات وتغييرها وبالتالي إمكانية تحويل الهجوم الالكتروني بعكس مساره.



رسم توضيحي 17: منظومة القيادة والسيطرة المعلوماتية

ومع تطور تقنيات الشبكات اللامركزية (peer-to-peer) أصبح القضاء على منظومة السلطة والسيطرة الالكترونية صعباً وهو يشتد صعوبة كلما تطورت معرفة الدول والمنظمات بالإمكانيات الهائلة لتكنولوجيا المعلومات والشبكات.

الإستراتيجية الدفاعية الإلكترونية

إن الإختراقات المعلوماتية التي تكاثرت في السنوات الأخيرة وسعي الدول الخارجية بشكل حثيث إلى إقتناء السلاح الرقمي الهجومي والتجسيي وسباق الاستحواذ على المهارات والكفاءات العاملة في هذا المجال يضع الحكومة الذكية أمام واقع دفاعي معلوماتي لا مناص من التهرب منه، ويبدأ الدفاع الوطني المعلوماتي أن تقوم الحكومة

برسم إستراتيجية دفاعية معلوماتية تنبثق عن الإستراتيجية الكبرى للدفاع الوطني وتحتوي على القدرات الالكترونية الهجومية والدفاعية على حد سواء المتوفرة للدولة وأجهزتها وترسانة السلاح الرقمي التي يجب تأمينها والتدرب عليها والتحالفات مع الدول والمنظمات والقوة البشرية المنوط بها إدارة الحرب الالكترونية أو تولي الدفاع الالكتروني عن أنظمة ومعلومات الدولة والقطاع الخاص وكشف المتسللين وسارقي البيانات الحكومية والتدرب على تقنيات البحث الجنائي الالكتروني. ومن سوف يتولى إدارة المعركة الالكترونية والتنسيق بين الوحدات التجسسية والهجومية والدفاعية.

وتعتني الإستراتيجية الدفاعية الالكترونية أيضاً بوضع أسس وكيفيات دراسة ملفات الاشخاص المخولين بالولوج إلى أنظمة ومعلومات الدولة والاتصالات والمكالمات والخرائط الجغرافية الالكترونية وكيفية إعطائهم حق الدخول (Access Control) ومتى يجب نزع هذا الحق عنهم وفي أية ظروف ومتابعة تعديلاتهم في الانظمة وتسجيل أوقات دخولهم والمعلومات التي اطلعوا عليها في أي زمان كان. وإذا كانت الحرب التقليدية قد اعتمدت إلى حد كبير على مفهوم الردع ينبغي التفكير ملياً بدراسة إمكانية الردع الالكتروني بحيث لا يفكر العدو في اختراق أنظمة الحكومة ومعلوماتها أو التلاعب بها، وعلى كل حال فإن الردع الالكتروني ما زال في طور الدراسات والبحوث ومعرفة إمكانية وجود ردع حقيقي في العالم الافتراضي ففي الحرب العسكرية تصل قذيفة المدفع أو الصاروخ إلى هدفها مدموغة بعنوان الرد والمرسِل بينما في الحرب الالكترونية يصعب التعرف مباشرة على من قام بالهجوم من أجل الانتقام منه وجعله يدفع الثمن.

ويجب أن تشتمل الإستراتيجية الدفاعية الالكترونية على القطاعات المدنية والاقتصادية والعسكرية على حد سواء، فكما يهدف الدفاع العسكري الى رد الأذى عن تلك القطاعات الثلاثة ينطلق الدفاع الالكتروني لكي يحمي الشعب من الخروقات الأمنية والثقافية ويحمي مؤسسات القطاع الخاص والبنوك ومصادر التمويل والشركات من التجسس الاقتصادي وكشف الاسرار التجارية والاختراعات، ويحمي المنظومة العسكرية والأمنية للدولة من التشويش أو التعطيل او التجسس خلال الحرب المشتعلة أو الباردة. وليس بالضرورة أن تقوم الحكومة بتجنيد العشرات من جنود الإنترنت من أجل حماية مصالحها ومصالح مواطنيها على الإنترنت بل من الممكن أن يكون الدفاع الالكتروني مقسماً على مستويات فالمستوى الشعبي تبذل فيه الدولة جهدها من أجل توعية المواطن ونشر المعرفة الأمنية في المدارس والجامعات حتى يعرف الشعب كيف يتصدى للإختراقات الثقافية والعقائدية التي يواجهها بنفسه وتتولى الدولة مسؤولية قائد الاوركسترا في هذا المجال بينما ينطلق آلاف المواطنين الذي يقضون وقتهم على الإنترنت من أجل المشاركة بفعالية في عملية الدفاع الشعبي الالكتروني ومن المهم أن تعمل الدولة على إظهار أن هذا الدفاع هو موضوع وطني والمشاركة فيه من الواجبات فلا يجوز أن تجتاح الإنترنت آلاف الدراسات والتعليقات والمقالات التي تضع الحق في ميزان العدو بينما يقضي شبابنا وقتهم على الفايسبوك في تبادل الصور والمحادثة. وبالنسبة للدفاع الالكتروني الشعبي فلا تحتاج الدولة الى استثمار في هذا المجال فقد تم بناء البنية التحتية للشبكات الاجتماعية العالمية ومواقع الأخبار والتعليقات ومن الممكن استغلالها في هذا المجال عبر توجيه المواطنين وفرق الدفاع الشعبي الالكتروني إلى مواضيع محددة تخدم

رسالة الوطن خلال الحرب أو السلم وإرشادهم بطرق بسيطة جداً كيف يستخدمون تلك الأدوات بطريقة مناسبة.

أما على المستوى الاقتصادي، فهل تتحمل مؤسسات المال والبورصات ومواقع الأخبار والتلفزيونات قطع بثها عن الإنترنت عبر هجوم إلكتروني مكثف؟ وقد حدث هذا الأمر في استونيا وجورجيا وهو ليس من نسج الخيال العلمي إنه حقيقة واقعة كلفت القطاعات الإقتصادية في تلك الدول ملايين الدولارات من الخسائر جراء انفصالها عن العالم الالكتروني لأيام، اما بالنسبة للبلدان العربية نحن نرى كيف يتم التقدم نحو الاقتصاد الرقمي بصورة حثيثة ويتم صرف الأموال في هذا المجال ولكننا لم نرى حتى اليوم بوادر دفاعية حقيقية تحمي مكونات ذلك الاقتصاد الرقمي من التداعي تحت ضربات العدو الالكترونية وبناءً عليه يصبح من الضرورة بمكان وجود استراتيجية دفاع إلكترونية تحمي المصالح الاقتصادية في البلد كواجب وطني. وعلى صعيد الدفاع الالكتروني العسكري فهو ينقسم إلى شطرين: الشطر الأول يعتني بالدفاع عن منظومة السلطة والسيطرة للدولة والتأكد من أن أجهزتها الالكترونية والاستشعارية وراداراتها الكاشفة للطائرات الحربية تعمل بجدارة على مدار الساعة من دون إمكانية إختراقها أو تعطيلها من قبل العدو ويعالج الشطر الثاني موضوع التجسس والوقاية الأمنية الالكترونية من أجل التأكد ان أجهزة الامن والمخابرات في الدولة لا تتعرض لإختراق أمني إلكتروني داخلي أم خارجي على حد سواء وذلك عبر تحديد المسؤوليات والأدوار والمعلومات التي يتم تداولها وتشفيرها عند نقلها أو تخزينها والمحافظة عليها في حال وقوع ضرر مادي في الاجهزة التي تحملها.

	الدفاع الشعبي الالكتروني	الدفاع الاقتصادي الالكتروني	الدفاع العسكري الالكتروني
القيم المهددة	الثقافة، التراث، اللغة، الدين، الشباب، الاخلاق	التنافسية، الجودة، سرعة المعاملات، التفوق الاقتصادي، النمو والتطور، الاختراعات والأصول الفكرية	العقيدة العسكرية، الكبرياء العسكري، ميزان الرعب، ثقة الشعب بالجيش والأمن.
اهداف الهجوم العدوانية	نشر الانحراف، تشكيل خلايا الكترونية مناوئة للدولة، الحصول على معلومات عن الافراد، التحريض على العنف، الدعوة الى العصيان المدني، تشكيك الشعب بمقدراته، بث أخبار وتقارير تضليلية، محاولة تجنيد عملاء وجواسيس عبر الإنترنت.	تدمير المنظومة الاقتصادية الالكترونية، سرقة الأموال، تدمير التجارة الالكترونية، إرباك التصدير والاستيراد، تهميش السياحة، تعطيل المعاملات الحكومية الالكترونية، إلحاق الخسائر المالية بالاقتصاد	شل منظومة السلطة والسيطرة، الحصول على معلومات امنية، الحصول على معلومات عن مستوى التسليح ونوعيته، التشويش على اجهزة الاستعشار والرادارات، إمكانية إعادة توجيه الصواريخ والقنابل الذكية، التجسس على الاتصالات، بث معلومات تضليلية.
استراتيجية الدفاع الوطنية	توعية الهيئات الشعبية والتجمعات الوطنية على الإنترنت، تشكيل لجنة وطنية توجه وتركز الدفاع	ضرورة توعية المدراء بمخاطر الحرب الالكترونية، إجراء عملية تقييم أمني معلوماتي لمصادر	الهجوم الالكتروني المضاد، محاكاة عملية اختراق امني معلوماتي، التاكد من ولاء الاشخاص المسؤولين

	الدفاع الشعبي الالكتروني	الدفاع الاقتصادي الالكتروني	الدفاع العسكري الالكتروني
	الشعبـــي الالكتروني وتخطط له.	وأصول الشركة الالكترونية، الحرص على استمرار العمل إذا انقطع الاتصال بشبكة الإنترنت محلياً.	عن المعلومات والأجهزة، عدم الاعتماد على وسيلة الكترونية واحدة، تحقيق الكتروني دوري حول من استفاد ويستفيد من المعلومات ولأية اسباب، تطوير ترسانة السلاح الرقمي، المرتزقة الالكترونيون!
أدوات الدفاع الالكتروني	الشبكات الاجتماعية الالكترونية، البريد الالكتروني، المنتديات المحلية والأجنبية، مواقع وسائل الإعلام، التصاميم والرسوم الوطنية الالكترونية، مواقع المدونين، كتيبات الحماية الالكترونية المختصرة العائلية والشخصية التي تصدرها الدولة.	برامج الحماية من الفيروسات، إدخال ثقافة أمن المعلومات الى الشركات، حماية الشبكات عبر أنظمة جدار النار واكتشاف المتطفلين، الاحتفاظ بنسخ إضافية عن المعلومات المهمة، تجهيز أكثر من موقع انترنت احتياطي، تجهيز بريد الكتروني للطوارئ خاص بالعاملين وغير منشور على الإنترنت.	برامج وأنظمة الحماية، التاكد من أن الشيفرة البرمجية للأنظمة المستخدمة لا تحتوي على أبواب تجسسية، التأكد من أن العتاد الالكتروني والاتصالاتي لم يتم التلاعب به، تجهيز منصات هجوم الكتروني ووضعها بتصرف القيادة، توظيف الخلايا الشعبية الالكترونية في الهجوم على مواقع العدو، نشر البرامج التجسسية

	الدفاع الشعبي الالكتروني	الدفاع الاقتصادي الالكتروني	الدفاع العسكري الالكتروني
			الوقائية، برامج المصيدة الالكتروني (Honeypot)
المسؤول عن الدفاع	كل من هو قادر على حمل السلاح الرقمي	مديرية المعلوماتية في المؤسسات	وحدات خاصة تقوم بإحداثها الدولة داخل الجيش والمخابرات

جدول 7: استراتيجية الدفاع الالكتروني في الدولة

إن العالم الالكتروني اليوم يضع الحكومة العربية أمام تهديدات حقيقية من ضمنها استغلال العدو لهذه الجبهة لإحراز تفوق استخباري ومعلوماتي ولكنه في نفس الوقت يعطي تلك الحكومات العربية الفرصة الذهبية ولأول مرة في تاريخ الصراع أن تواجه أعداءها بنفس المستوى من التسليح الرقمي ونفس الكفاءات والقدرات ويقدم لتلك الدول الفرصة أيضاً لإحراز نصر مباشر وواضح من خلال توفّر الأدوات وسهولة الإستحواذ عليها.

ترسانة السلاح الرقمي

من المعلوم أن أية حرب من الحروب سواءً كانت عسكرية مادية أو إلكترونية رقمية بحاجة إلى عدة عناصر مجتمعة من اجل إطلاقها وإدارتها ويعتمد النصر فيها أو الهزيمة على عدد من الاستراتيجيات والتكتيكات وعلى العنصر البشري وأهم من كل ذلك على ترسانة السلاح المتوفرة بيد ذلك العنصر البشري، والحرب الرقمية لا تختلف كثيراً في هذا المجال حيث انها تعتمد على التخطيط والإستراتيجية والتنظيم والتدريب وعلى ترسانة

سلاح من نوع آخر: إنها ترسانة السلاح الرقمي. ونحن نتحدث هنا عن اشتبكات رقمية معلوماتية محترفة ومنظمة وليست من قبيل تلـــك الـــتي يقودها الهواة ويحاولون الحصول على بعض الـــبرامج عـــن الإنترنـــت واستخدامها، إن الدول الكبرى اليوم بدأت ببناء ترسانة سلاح رقمـــي بكل ما للكلمة من معنى وهي تسعى أن تكون تلك الترســـانات ســـرية وجاهزة لدعم ومؤازرة أي حرب أو اشـــتباك سياســـي أو عســـكري مستقبلي، ولا تقتصر ترسانة السلاح الرقمي علـــى أســـلحة التعطيـــل والتخريب بل تتعداها إلى الاسلحة التجسسية وأدوات ووسائل محاربـــة الاعتراضات والتجمعات الالكترونية ضد الدولة وإلى ما هنالك.

	السلاح الرقمي	السلاح التقليدي
خسارة الأرواح	محدودة	عالية جدا
المدى بالكيلومتر	تطال أية نقطة وصلت اليها الإنترنت – حتى الفضاء	يعتمد على نوعية السلاح – محدود يقاس بالكيلومترات
التأثير بالرأي العام	عالي	منخفض
الحرب النفسية	عالية	عالية
كلفة الاقتناء والصيانة	منخفضة	عالية
الاستخدام للتجسس	عالية	منخفضة
عدد مرات الاستخدام	مرات عديدة – طالما بقي السلاح الرقمي تحت سيطرة القيادة	مرة واحدة – إطلاق ثم تفجير
المهارات البشرية المطلوبة	مهارات ناعمة	مهارات خشنة

جدول 8: السلاح التقليدي مقابل السلاح الرقمي

وعلى سبيل المثال فقد ذكر موقع تقنيات الدفاع الالكتروني عن روسيا وحدها أنها قد خصصت ميزانية ما يقارب 130 مليون دولار سنوياً لقدرات الدفاع والهجوم الالكتروني ويقول الموقع في إحدى دراساته أن روسيا تتمتع بالترسانة الرقمية التالية (المعروفة والغير سرية):

- شبكات ضخمة من البوتنت منتشرة في العديد من البلدان تستطيع استخدامها من أجل إطلاق هجوم تعطيل خدمات المواقع والتجسس الرقمي المعلوماتي
- اسلحة كهرومغناطيسية من أجل تعطيل المعدات وأجهزة الاتصال والشبكات
- برامج مزيفة تحتوي على فيروسات انتشار ذاتي
- أنظمة متقدمة للكشف عن الثغرات في مواقع العدو الالكترونية وتوظيفها
- أنظمة للتجسس على الشبكات اللاسلكية وتعطيلها ايضاً
- قنابل رقمية كامنة تنتظر ساعة الصفر من أجل تخريب شبكات البنى التحتية للعدو
- مجموعة كاملة من فيروسات الكمبيوتر وقدرة على انتاجها وإخفائها والاستفادة منها
- مجموعة متقدمة من أنظمة الاستطلاع الالكتروني وتجميع المعلومات وتحليلها.

وبالتأكيد فإن معظم الدول التي تبني قدرات حربية إلكترونية فإنها لا تعلن عنها ولا تحاول استخدامها في غير محلها أو غير وقتها حتى لا يتم كشفها وبالتالي التعامل معها والتحضير لمواجهتها في أية حرب إلكترونية مستقبلية.

تطبيقات حكومية ذكية

في هذا الفصل سوف نشرح بعض التطبيقات الذكية في مجال العمل الحكومي أو البلدي والتي قامت بتطبيقها بعض البلدان بنجاح، علماً أننا التطبيقات الذكية المحتملة كثيرة ولا مجال لحصرها ولكن جميعها سوف تتشابه من حيث التقنيات والإمكانيات وطريقة طلب الخدمة ولذلك يمكن للقارئ أن يقوم بتطبيق نفس المعايير على تطبيقات جديدة قد تكون موضع حاجة لدى حكومته أو إدارته المحلية.

ومن الممكن تقسيم التطبيقات الذكية إلى عدة أقسام من أجل تسهيل العملية على صاحب القرار وتحديد المسؤوليات والصلاحيات ونقترح التقسيم التالي:

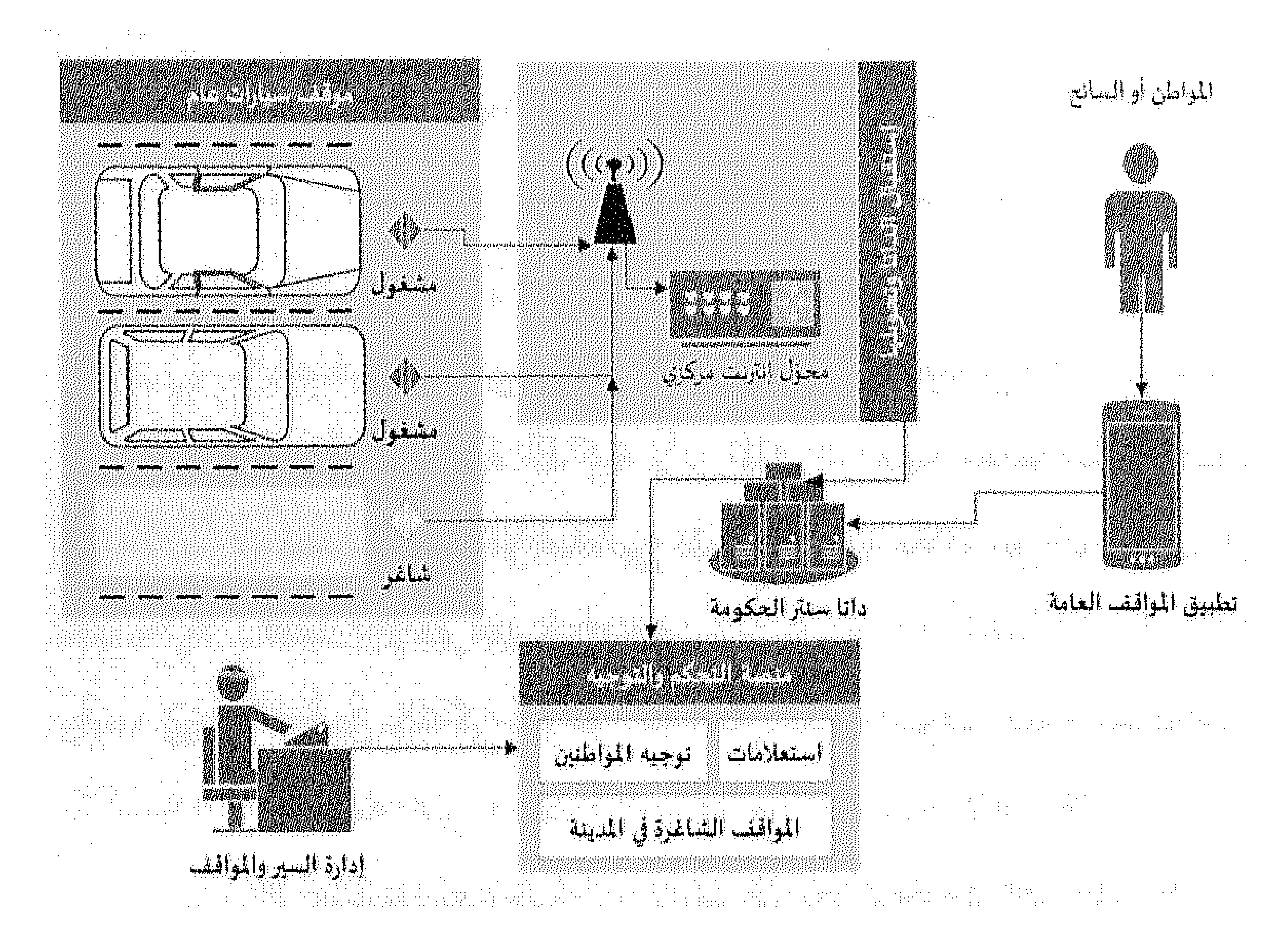
- **تطبيقات المدينة الذكية**: وعادةً ما تكون مسؤولية البلديات المحلّية ومنها تطبيقات المواقف العامة وتطبيقات إدارة مستوعبات النفايات وإشارات المرور الضوئية وأنظمة الريّ الذكية ومجسّات قياس الإزدحام المروري.
- **تطبيقات الحكومة الذكية المشتركة**: وهي التطبيقات المركزية التي تنشرها الحكومة وتكون مشتركة بين كل القطاعات ومنها نظام تسديد الرسوم عبر الجوّال ونظام تحديد هوية المستخدم ونظام الإشعارات.
- **تطبيقات الأمن الذكي**: وهي التطبيقات التي تخدم سلامة المواطنين ومحاربة الجريمة والإرهاب ومنها شبكات

كاميرات المراقبة الرقمية وتطبيقـــات التواصـــل الأمـــني والمعلوماتي بين المواطنين والحكومة والتبليغ عن التهديـــد والمخاطر.

- **تطبيقات الخدمات الحكومية:** وهي التطبيقات التي تعـــنى بخدمات الحكومة العامة ومعاملاتها وتجديد الوثائق وتغـــيير عناوين السكن ورخص القيادة وجوازات السفر وخدمات مختلف الوزارات بشكل عام.
- **التطبيقات الخدمية العامـــة:** ومنـــها تطبيقـــات المنـــاخ والفعاليات والنشاطات واســـعار العمـــلات والمؤشـــرات الإقتصادية وحركة الطيران والبواخر ومؤشرات التلوث.

المواقف الذكية في المدينة

يساعد هذا التطبيق البلديات المحلية وإدارة المدن علـــى توجيـــه السيارات إلى أماكن الوقوف الشاغرة في المدينة من خـــلال تركيـــب أجهزة إستشعار في المواقف العامة وعندما يصبح المكـــان شـــاغراً أو محجوزاً يتم إرسال تلك المعلومات إلى سيرفيرات البلدية الذكية والـــتي تنشر تلك المعلومات بطريقة لحظية على تطبيقاتها الجوالة مـــن أجـــل إرشاد المواطن إلى أمكنة ركن السيارات الشاغرة وكيفية الوصول إليها وعبر أية طريق والوقت المتوقع للوصول خلال الازدحام العـــادي أو الازدحام الشديد.



رسم توضيحي 18: المواقف الذكية في المدينة

ويمكن مساعدة المواطن مباشرة من خلال الاتصال بهاتف مركز المساعدة أو عبر تطوير تطبيق ذكي على الهواتف الجوّالة يقوم بالتعرف على مكان المواطن الجغرافي من خلال خاصية ال جي بي أس (GPS) وعرض المواقف الشاغرة في محيط جغرافي حول المكان الذين يتواجد فيه.

تطبيق الوظائف الحكومية

ويمكن من خلال هذا التطبيق أن تنشر الحكومة، بمختلف وزاراتها وإداراتها العامة، معلومات عن الوظائف الشاغرة فيها وشروط التقدم للوظيفة والشهادات المطلوبة وإذا ما كان هناك إمتحان جدارة أو مباراة للفوز بتلك الوظائف. وينقسم التطبيق إلى شقين رئيسيين:

1. الواجهة الخلفية: من أجل إدارة الوظائف وتعديلها والموافقة على نشرها أو إزالتها أو الإعلان عن ملئهـــا، ويمكـــن أن تكون منصة الإدارة الخلفية عبارة عن تطبيق وب يعمل على المتصفحات من خلال الأجهزة المكتبية وليس بالضرورة من خلال الأجهزة الذكية لأن تلك الواجهة ســـوف تكـــون مقتصرة على الأشخاص المخولين بالإعلان عن الوظائف في مختلف الإدارات الرسمية.
2. التطبيق الذكي: وهو البرنامج الذي سوف يقوم المـــواطن بتحميله على جهازه الجوّال من أجـــل الإطـــلاع علـــى الوظائف المعروضة أو الإشتراك بالإشعارات التي يتم بثهـــا عند نشر وظائف جديدة.

خصائص النظام

من أجل أن يكون النظام فعّالاً من المهم أن تكون عملية البحث عن الوظائف فيه سهلة ومن الممكن إستعراض وظيفة معينة عبر أحـــد الإمكانيات التالية:

1. إستعراض جميع الوظائف الشاغرة في مختلف أجهزة الحكومة مع إمكانية التصفح بشكل صفحات متتالية
2. البحث عن وظيف حسب مفردات مفتاحية (Keywords)
3. إستعراض الوظائف ضمن تصنيف وظيفي معـــين مثـــل: المحاسبة، المعلوماتية، إلخ...
4. إستعراض الوظائف حسب الجهة التي تقدمها مثل الوظائف التي تقدمها أجهزة الأمن العـــام أو وزارة الطاقـــة أو وزارة السياحة وغيرها من الإدارات العامة

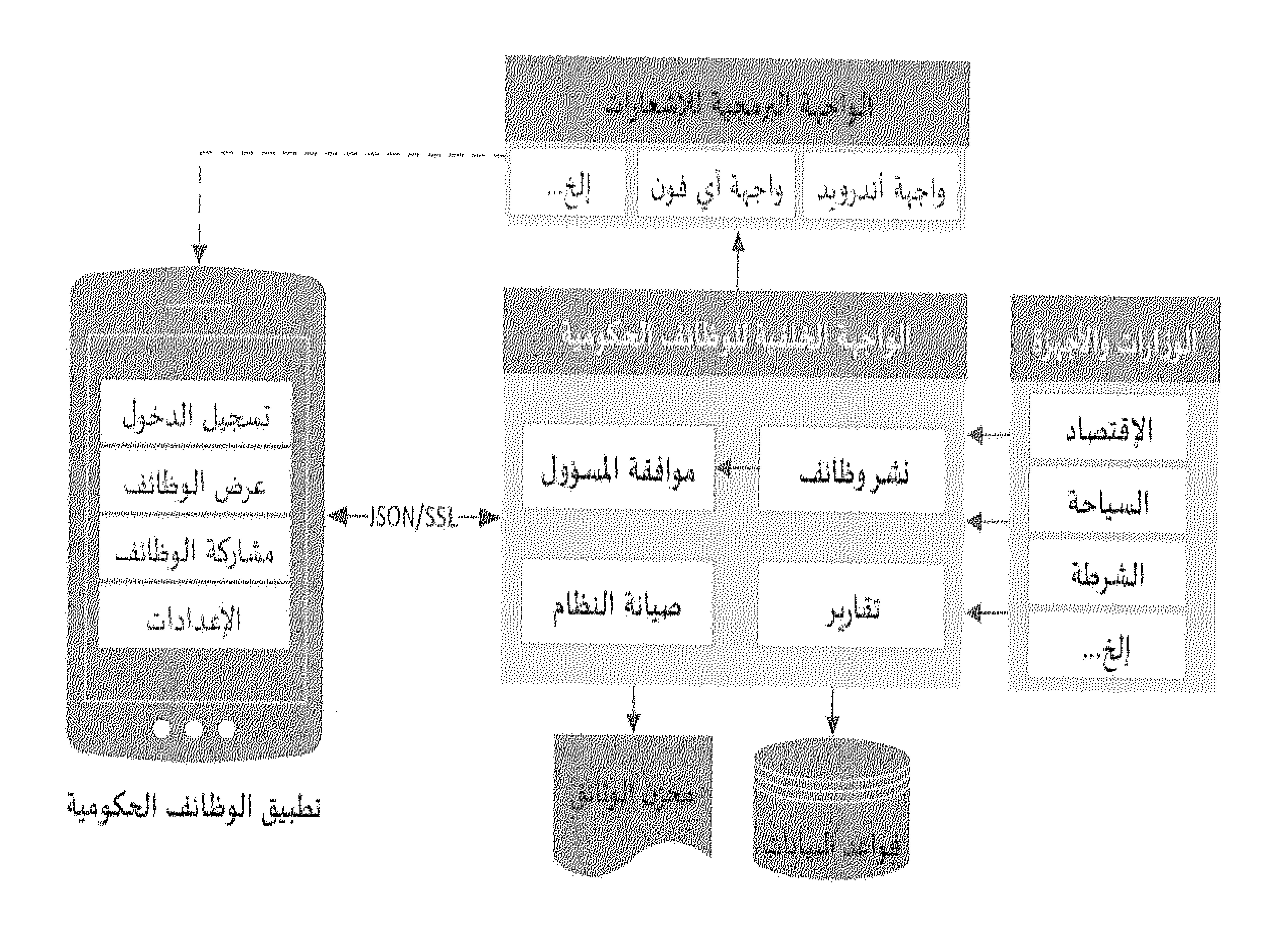
ومن الخصائص المهمة للتطبيق هي تمكين المستخدم من الاشتراك بالإشعارات حول الوظائف الجديدة في تصنيف معين أو وزارة معينة وعندما تنشر تلك الوزارة وظيفة شاغرة يتم إرسال رسالة تلقائية إلى المستخدم تعلمه فيها عن تلك الوظيفة من دون أن يرجع كل يوم ويبحث في التطبيق.

كما يمكن للتطبيق أن يتيح للمستخدم إمكانية "متابعة Follow a Job" وظيفة شاغرة معينة حتى يتم إعلامه تلقائياً بمواعيد التقدم بالطلبات ومواعيد مباراة القبول الخاصة بتلك الوظيفة على سبيل المثال. ويمكن للتطبيق أيضاً ان يمكّن المستخدم من مشاركة معلومات وظيفة معينة مع شبكة أصدقائه (Job Information Sharing).

الواجهة الخلفية للنظام

بما أن هذا النظام سوف يخدم جميع الأجهزة الحكومية والوزارات ينبغي التأكد من عدة أمور تقنية وإدارية وتضمينها في الواجهة الإدارية الخلفية ومنها:

1. التأكد من إستحالة عبث جهة معينة بمعلومات وظائف جهة أخرى عن طريق الخطأ او العمد
2. تضمين نظام سلسلة الموافقة الإدارية (Workflow) في النظام من أجل التأكد من موافقة المسؤول في الوزارة على المعلومات التي يدخلها موظف الداتا قبل نشرها
3. إمكانية تحميل مرفقات خاصة بالوظيفة من قبيل المستندات والوثائق المساعدة
4. إمكانية إصدار تقارير إدارية عبر واجهة التحكم الخلفية



رسم توضيحي 19: التطبيق الذكي للوظائف الحكومية

وتسمح لنا هذه المعمارية بإضافة وتعديل الجهات المقدّمة لخدمات الوظائف والتي سوف يتولاها مدير النظام حيث يكون من مهامه إدخال جهات حكومية جديدة وتعديل معلوماتها وتعيين مستخدم مخول بإدخال معلومات تلك الجهات وكذلك يتولى مدير النظام عملية إدخال التصنيف الوظيفي وتعديلاته والكثير من وظائف الصيانة والتقارير.

تطبيق المواطن المسؤول

يشجّع هذا التطبيق المواطن على أن يكون مشاركاً في المسؤولية المجتمعية عبر إرسال معلومات وصور حول الأعطال والتعديات على الشبكات العامة والحفر في الطرقات والمخالفات المرورية والاشتباهات الأمنية وكل ذلك عبر هاتفه الجوّال الذي يسمح له بإلتقاط الصور

وتحديد المكان الجغرافي الحالي لموضوع التبليغ. ومن الممكن أن تستقبل البلديات المحلية التبليغات الصادرة من المواطنين وتحويل التبيلغات الأمنية للجهات المختصة بالدولة.

وبالتالي المعلومات التي من الممكن أن يقوم المواطن بإرسالها:

إستمارة حالة في تطبيق المواطن المسؤول		
عنوان الحالة	مثلاً: تضرر في خطوط شبكة الكهرباء	
تفاصيل الحالة	نص صغير يشرح فيه المواطن تفصيل الحالة	
صور الحالة	إلتقاط الصور وتحميلها مباشرة مع الاستمارة	
إحداثيات الحالة	المكان الجغرافي للحالة	
نوع الحالة	• حالة أمنية • سرقة أو إعتداء • عطل في البنية التحتية	• مخالفات مرورية • حرائق • حفر في الطريق

جدول 9: استمارة تطبيق المواطن المسؤول

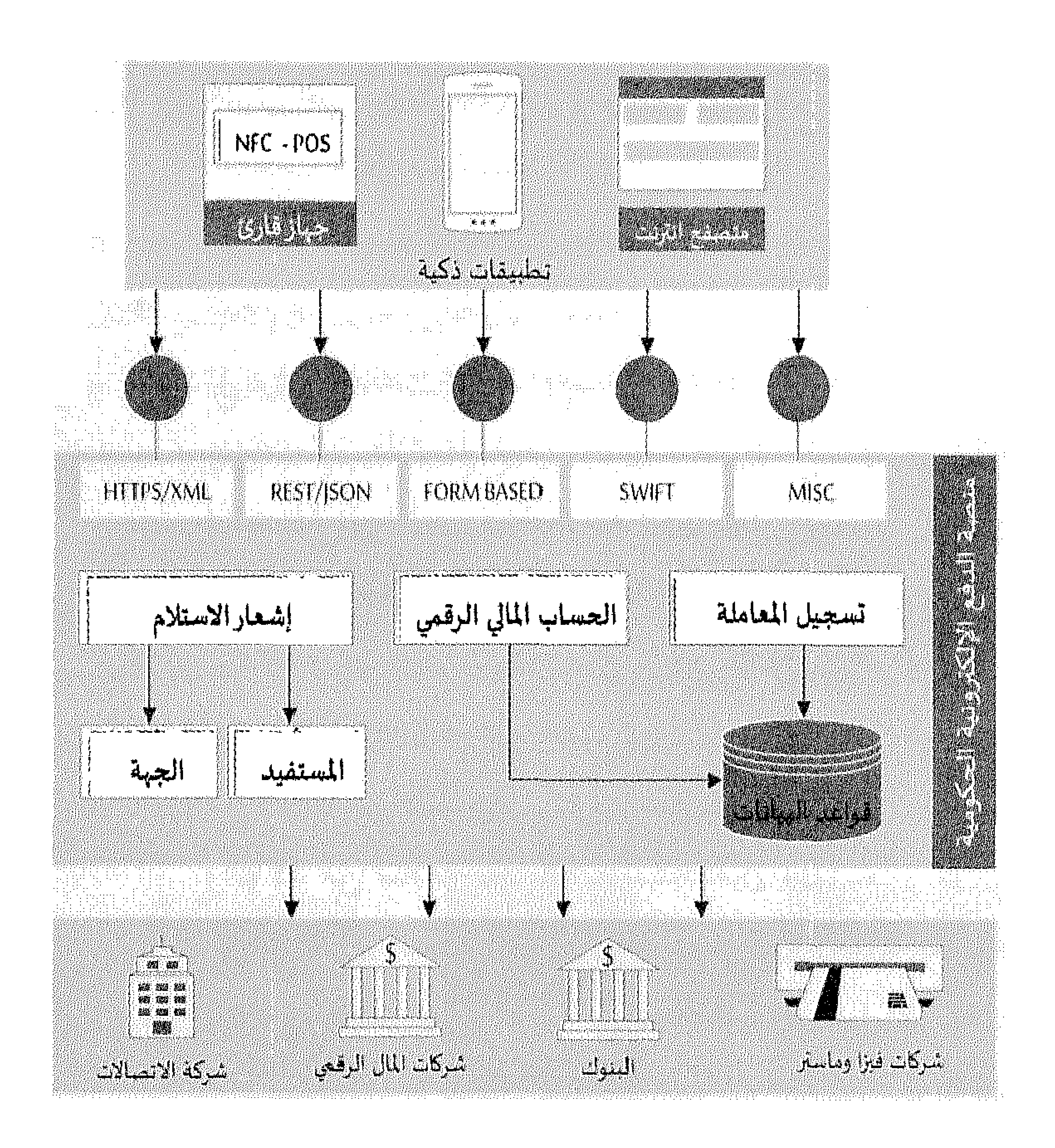
منصة الدفع الالكترونية الحكومية

مع نقل الخدمات الحكومية إلى أجهزة الجوّال ومن أجل إكتمال الصورة من الضروري أن تتوفر إمكانية تسديد الرسوم عبر تلك الأجهزة فمن غير المنطقي أن يباشر المواطن تنفيذ خدمته الحكومية عبر جهازه الذكي ثم ينتقل لكي يسدد الرسوم يدوياً أو عبر تحويلات بنكية أو غيرها من وسائل الدفع التقليدية. وعلى سبيل المثال، قد تتوفر خدمة مراجعة مخالفات المرور عبر تطبيق خاص بالأجهزة الجوّالة والذكية ومن

خلالها يتمكن المواطن من معرفة ما إذا كان هناك مخالفات مرورية بحقه ولكن لن يكون هذا التطبيق فعّالاً إذا لم يتمكن المواطن من تسديد رسوم تلك المخالفات إلكترونياً من دون تكبد العناء والذهاب شخصياً إلى مكاتب إدارة السير أو المكاتب المعتمدة لديها.

ومن المؤكّد أن إطلاق يد الوزارات والإدارات العامة الحكومية في بناء أنظمة دفع إلكترونية حسب ما تراه مناسباً سوف يوقع الحكومة في الكثير من المشاكل التقنية والمالية والإدارية عدا عن إمكانية توفّر الموارد البشرية والمادية لذلك، كما أن ذلك الأمر سوف يهدر الكثير من الطاقات الحكومية عبر تكرار نفس العمل في مختلف الإدارات وإن بنسب متفاوتة في الإحتراف والتميز.

وبناءً على ما تقدم، يبقى الحل الأمثل للحكومة هو بناء منصة دفع إلكتروني مشتركة تعتبرها خدمة من خدمات البنية التحتية للحكومة الذكية وتقوم مختلف الوزارات والإدارات بتوظيف تلك الخدمة داخل تطبيقاتها الذكية من أجل تسديد الرسوم مركزياً على أن يصار إلى فرز العوائد المالية دورياً حسب الجهة الحكومية صاحبة الرسوم في المقام الأول.



رسم توضيحي 20: منصة الدفع الالكتروني الحكومية

ومن إجل إكتمال الصورة نذكر بعض الوسائل المحتملة التي يمكن للحكومة من خلالها تقاضي رسوم الخدمات إلكترونياً ومنها:

- بطاقات الإئتمان وذلك عبر التعاون مع البنوك المحلية من أجل تصفية حسابات الدفعات، علماً أن ليس غالبية المواطنين يحملون تلك البطاقات أو يعتمدون عليها.
- بطاقات المال الالكتروني ومثال على ذلك الدرهم الإلكتروني في دولة الإمارات العربية المتحدة حيث يشتري المواطن بطاقة

تحتوي على رصيد مالي من الدراهم ويقوم بصرفه على الخدمات الحكومية وبذلك لا يحتاج إلى حيازة بطاقة إئتمان وتكون الحكومة قد قبضت سلفاً على خدمات لم تقدمها بعد!

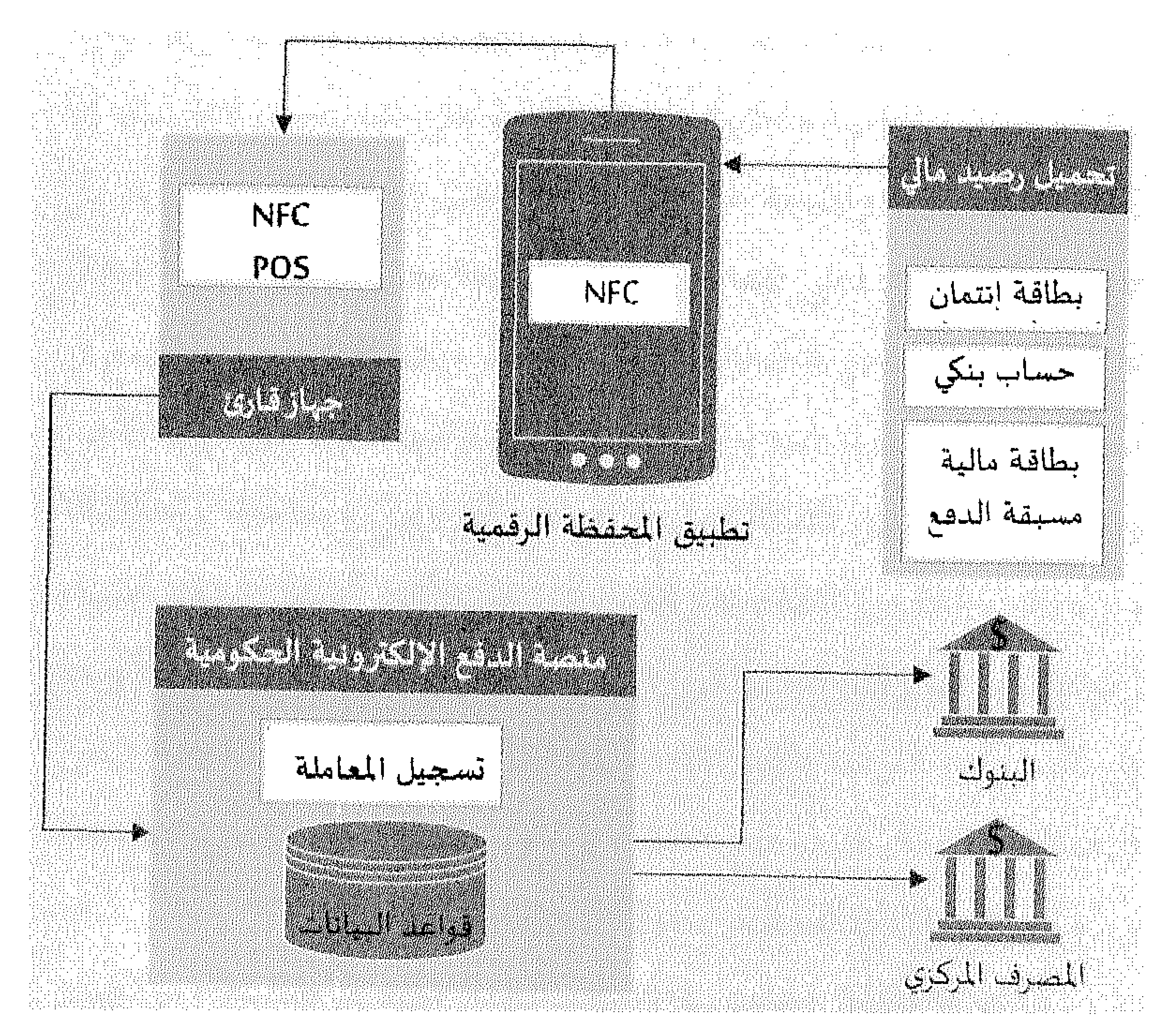
- الدفع عبر رسائل الجوّال النصية عبر إرسال قيم المبلغ المالي إلى رقم تخصصه شركة الإتصالات لبعض خدمات الحكومة ويتم حسم ذلك المبلغ من رصيد المشترك وتسديد المبالغ المستحقة إلى الأجهزة الحكومية المعنية بعد حسم رسوم المعاملات لصالح شركات الإتصالات.
- إستخدام خدمات وسطاء المال الرقمي مثل شركة Paypal وشركة Scrill وغيرهم حيث يمكن للحكومة فتح حسابات مع تلك الشركات والتي تتولى عملية تطوير الأنظمة والتأكد من سلامة معلومات المستخدمين وفقاً لمعايير الأمن العالمية للمال الرقمي وحفظ داتا المشتركين بينما تقوم الحكومة فقط بإستخدام واجهات التطبيق البرمجية المتوفرة من تلك الشركة داخل تطبيقاتها. وبذلك تكون الحكومة قد أزاحت عن كاهلها عبء تطوير النظام ومتابعة شكاوى العملاء وتأمين الداتا وكل ذلك عبر دفع رسوم مالية صغيرة لشركات المال الرقمي.

وتكمن أهمية بناء منصة دفع إلكترونية خاصة بالحكومة بغض النظر عن الحلول المطروحة أعلاه في أن الحكومة غالباً ما تريد بيانات وتقارير عن الحركة المالية لواردات خدماتها وهنا تأتي منصة المال الرقمي الحكومية لكي تمثّل بوابة موّحدة لتسديد الرسوم تتمكن من خلالها الحكومة من تسجيل كافة المعاملات الواردة إليها والجهة صاحبة الخدمة والمواطن طالب الخدمة والقيمة المالية والقطاع المعني بالخدمة

وبذلك تتمكن من إصدار تقارير مركزية لحظية حول حركة المال الرقمي الناتج عن النشاط الخدماتي الحكومي الإلكتروني

مع العلم أن الكثير من التقنيات الواعدة في مجال تحويل الهاتف الذكي إلى محفظة مالية رقمية قد بدأت حول العالم ولكن يحتاج إنتشارها إلى فترة من الزمن وذلك حتى تنتشر الأجهزة التي تحتوي على تقنية NFC على نطاق واسع وتشارك مؤسسات الأعمال في إستقبال دفعات مالية بتلك التقنيات.

ويبين النموذج التالي تركيبة الدفع الإلكتروني عبر الجهاز الذكي من خلال تقنية NFC (النموذج هو عبارة عن تصوّر عام وليس بالضرورة نموذج عملي حقيقي)



رسم توضيحي 21: محفظة النقد الرقمي

خاتمة الكتاب

في خاتمة هذا الكتاب أتمنى أن أكون قد أخذت المسؤول الحكومي ومدراء المعلوماتية فيها والمواطن وصاحب المؤسسة، على حدٍ سـواء، في جولة تقنية وإستراتيجية حول ما يحدث حولنا من تطـورات في مجـال تحديث العمل العام والخدمات الحكومية وحماية مصالح الدولة ومواطنيها في عصر الذكاء والمعرفة. وقد لا تستطيع معظم الحكومات العربيـة ان تقوم بتلك النقلة النوعية بطريقة مباشرة وكليّة نظراً لعدم تـوفّر المـوارد المالية والبشرية المناسبة ولكنها بالتأكيد قادرة على التدرج في التنفيـذ إذا كانت لديها رؤية واضحة عن المسار الذي يجب ان تسلكه مـن أجـل التحول الضروري لكي تتماشى مع متطلبات العصر الرقمي. ومن خلال تجربتي مع العديد من الكيانات الحكومية فقد وجدت ان معظمها يقع في فخ الجمود أمام دراسات وإستشارات تم إسقاطها عليها من دون الأخذ بعين الإعتبار معايير الثقافة وطبيعة المواطن العربـي وحاجاته وإمكانياته وأولوياته وبدلاً من التقدم بسرعة ووعي إلى الأمام نجدها تتجمد أمـام أكوام الأوراق والدراسات التي تنتهي في الجوارير المغلقة. ولذلك أتوجه إلى المسؤولين العرب بالقول أنه لم يعد الوقت مناسباً للحـديث عـن الاصلاح والتحديث ووضع الخطط بل أتى وقت التنفبذ الفعلي بحكمـة ومرونة وسرعة لأن العالم من حولنا لا ينتظر.

ولأن الأجهزة الحاسوبية والشبكات الرقمية الوطنيـة ومراكـز الداتا المحلية والسحابة الحاسوبية الحكومية والأجهزة الذكيـة وانظمـة

التحكم بشبكات الكهرباء (SCADA) والهاتف، كلها مع بعضها تمثل البنية التحتية للإقتصاد المعرفي في الدولة وحكومتها الذكية كان لا بد من الحديث بإسهاب عن الإجراءات الوقائية والدفاعية الالكترونية التي تتخذها أجهزة الدولة الأمنية من أجل الحفاظ على تلك الأجهزة والشبكات والداتا حتى لا تقع فريسة بأيدي المعتدين الخارجيين أو المخربين الداخليين.

في عصر المعرفة والذكاء، لا بد أن تكون الحكومة ذكية وعارفة بما يدور حولها محلياً وإقليمياً وعالمياً ومسلّحة بالأدوات الرقمية من رأسها إلى أخمص قدميها حتى تتمكن من ممارسة عملية الحكم بكفاءة وإلا فإن مصيرها إلى الفشل الذريع.

نحن لا نعرف كيف سيكون شكل الحكومة في المستقبل، ولا كيف سيكون شكل تلك الأداة التنفيذية التي تتولى إدارة شؤون البلاد والسهر على أمنها ولكننا نعرف بالتأكيد أنها لن تكون كما هي عليه اليوم!

المصطلحات

المصطلح	الشرح
واجهة التطبيقات البرمجية API	وهي البرامج القياسية التي تنشرها الحكومة او المؤسسة من أجل التواصل مع أنظمتها عبر مختلف لغات البرمجة
نظام تحديد الأماكن GPS	تحديد المكان الجغرافي وقد أصبحت معظم الأجهزة المحمولة الذكية تتضمن هذا النظام
العدّادات الذكية Smart Metering	وهي عدادات قراءة الخدمات المائية والكهربائية على سبيل المثال وإرسال الداتا مباشرة إلى الدوائر المختصة في الحكومة او أقسام الجباية
جهاز الاستشعار Sensor	أجهزة صغيرة تستطيع إلتقاط الداتا من المناخ أو الماء او جسد الإنسان (الحرارة، إلخ...)
البحث الفدرالي FEDERATED SEARCH	وهي عملية البحث في أكثر من نظام قد تكون موزعة على أكثر من منطقة جغرافية في نفس الوقت ويستخدم النظام "أكس كي سكور" هذه الخاصية.
مركز الداتا DATA CENTER	وهو المكان الذي يحتوي على أجهزة الكمبيوتر الخوادم (Servers) والشبكات ومعدات الشبكات وعادةً ما يكون الدخول إلى تلك المراكز محدداً بأشخاص معينين أو ضمن تصريحات ينتهي مفعولها في وقت زمني سريع.
الحوسبة السحابية CLOUD COMPUTING	وهي طريقة حديثة لنقل معظم التطبيقات إلى الشبكات العالمية المنتشرة على الإنترنت بحيث تكون "السحابة الحاسوبية" بمثابة داتا سنتر ضخم جداً يتم حجز أجزاء منه لصالح الشركات التجارية أو الحكومية. ويوجد الكثير من التفاصيل حول الحوسبة السحابية لا مجال لذكرها هنا.

BIG الداتا الضخمة DATA	بدأ هذا المصطلح بالظهور في السنوات الأخيرة مع الإنتشار الكثيف للشبكات الالكترونية الاجتماعية وما ينتج عن حركتها من حجم هائل للداتا نتيجة لتواصل الأفراد والمجموعات مع بعضهم البعض. وقد أثر ذلك الحجم على الطريقة التي نعالج بها المعلومات وظهرت الكثير نت التقنيات التي تعنى بمعالجة الداتا الضخة وإستخراج معلومات تحليلية منها.
VPN (Virtual Private Network)	الشبكة الافتراضية الخاصة وهي شبكة خاصة داخل شبكة الإنترنت تعتمد على تشفير مسار الداتا بين نقاطها
VPC (Virtual Private Cloud)	الكلاود الخاص وهو شبه مركز داتا إفتراضي خاص بالمؤسسات داخل الكلاود العام لأحد الشركات
SSL	بروتوكل التشفير بين طرفين بإستخدام الإجازات الرقمية
HTTP	بروتوكل نقل النصوص عبر خوادم الوب
JSON	النسق القياسي للداتا الذي إنتشر مؤخرا واصبح معتمداً في الواجهات البرمجية على الإنترنت
Service Availability	توافر الخدمة
Asynchronous Service	إمكانية طلب الخدمة والحصول على النتيجة لاحقاً خاصة مع الخدمات التي تأخذ وقتاً من أجل تنفيذها
ZigBee	بروتوكول الوايرلس الخفيف من حيث تردد حجم الداتا في الثانية
XBee	شرائح وايرلس جاهزة للشبك في الأنظمة الحاسوبية
Raspberry PI	جهاز كمبيوتر صغري من دون طرفيات وعادة ما يحتوي على نظام تشغيل لينكس ولغة البرمجة بايتون
Arduino	شريحة حاسوبية تحتوي على معالج وذاكرة وصول عشوائي ومنفذ داتا

Elastic Computing	الطاقة الحاسوبية المطاطة وتعني إمكانية إضافة أو تقليص عدد الخوادم الإفتراضية من خلال واجهة المدير او لغة البرمجة
GovCloud	الكلاود الخاص الحكومي (حتى الآن يطلق هذا الإسم على الكلاود الحكومي الأميركي)
الحقائق الأمنية Intelligence Facts	معظم المعلومات المفتوحة المصدر والناتجة عن الوسائل الإعلامية كالصحف والمجلات ونشرات الأخبار وتقارير الخبراء والمواقع الالكترونية الإجتماعية والمدونات قد لا تحمل معلومة أمنية دامغة ولكن دراسة التقاطعات بين تلك المعلومات ومقارنتها بأنماط عمل الهدف أو إيديولوجيته أو تدعيمها بمعلومات أمنية ثابتة وموثقة قد تؤدي إلى كشوفات جديدة.
معلومات المصادر المفتوحة	وهي المعلومات المتوفرة للجمهور وقد تكون مخفية في بعض الأحيان ولكنها ليست سرية.
التنصت الشامل Blanket Surveillance	عمليات التنصت الواسعة النطاق على الأهداف وغير الأهداف من أجل الحصول على أكبر كم من الداتا
البوتنت BOTNET	وهي شبكات من الفيروسات الموجهة من خلال منظومة قيادة وسيطرة حيث يتم التحكم بها عن بعد من أجل التجسس على أجهزة الكمبيوتر والأجهزة المحمولة.
التعرف على الأنماط Pattern Recognition	وهي عملية دراسة أحداث أمنية معينة سابقة على فترات زمنية متقاربة أو متباعدة من أجل إستنباط أحداث أمنية قد تحدث في المستقبل.
QR Code	رمز مرئي عادة ما يكون على شكل صورة من الخطوط المتقاطعة والتي تستطيع الأجهزة قراءتها وإستخراج المعلومات منها مثل عناوين المواقع وغيرها.
Multi-factor Authentication	التعرف على المستخدم من خلال أكثر من عاملٍ، مثلاً: كلمة السر والبصمة البيومترية معاً.

المراجع

مواقع الإنترنت

http://www.supermonitoring.com/blog/2013/09/23/state-of-mobile-2013-infographic/
http://gigaom.com/2011/10/13/internet-of-things-will-have-24-billion-devices-by-2020/
http://www.businessinsider.com/smartphone-and-tablet-penetration-2013-10
http://mashable.com/2014/01/21/whatsapp-doubles-users/
http://aws.amazon.com
http://topics.nytimes.com/top/reference/timestopics/subjects/c/cyberwarfare/
http://www.theguardian.com/world/the-nsa-files
http://www.aljazeera.net/books/pages/3639af79-1033-45d5-831f-66b36bb9e880

* تم سحب معلومات الإنترنت في الروابط أعلاه بين ايلول 2013 وشباط 2014

الكتب والدراسات

1. Gautam Shroff, The Intelligent Web, Oxford University Press, UK, 2013
2. Honb Zhou, The Internet of Things in the Cloud, CRC Press, USA, 2013
3. Michael Graves, Digital Archeology, Addison Wesley, USA, 2014
4. Michael Hugos and Derek Hulitzky, Business In the Cloud, Jon Wiley and Sons, USA, 2011
5. P.W. Singer and Allan Fiedman, Cybersecurity and Cyberwar, Oxford University Press, USA, 2014
6. Stefan Sjogelid, Raspberry Pi for Secret Agents, PACKT Publishing, UK, 2013
7. عباس بدران، الحكومة الالكترونية من الإستراتيجية إلى التطبيق، المؤسسة العربية للدراسات والنشر، لبنان، الطبعة الأولى 2004

حول المؤلف

عباس بدران مدير مؤسسة إيكونسبت الاستشارية (مركز دراسات الحكومة الالكترونية) في بيروت- لبنان هو مؤلف كتاب الحكومة الالكترونية من الاستراتيجية إلى التطبيق وكذلك كتاب الحرب الالكترونية - الاشتباك في عالم المعلومات. وقد عمل السيد بدران في العديد من الشركات العالمية في قطاع المعلومات ومنها شركة ترنسورلد العالمية في وادي السيليكون في كاليفورنيا وكذلك قدم الاستشارات المعلوماتية للعديد من الشركات في الخليج العربي ومنها شركة النفط السعودية ارامكو وشركة أدكو في الامارات العربية المتحدة. عمل سابقاً بصفة مستشار وزير الاقتصاد والتجارة اللبناني السابق الدكتور ناصر السعيدي حيث تولى مسؤولية الارتباط المعلوماتي في لبنان مع دول شرق المتوسط من ضمن مشاريع الإتحاد الاوروبي.

له عشرات المؤلفات والمقالات في مجال تطوير الحكومة الالكترونية وأمن المعلومات وتحديث الإجراءات والشبكات الاجتماعية الالكترونية ومعظمها منشورة على الموقع الالكتروني التابع للمركز.

هذا الكتاب

يعالج المؤلف في هذا الكتاب موضوع تطوير الحكومة الإلكترونية من أجل إضفاء لمسة من الذكاء عليها، حيث أن الحكومة الذكية سوف تمثل النموذج الأنجح للحكومات القادرة على الإستمرار في عملية الحكم في العقود المقبلة. لقد تغيّرت التحديات خلال عقد من الزمن وإنتشر الإجرام الإلكتروني والبلبلة وفوضى السايبر وذابت حدود الدولة في العالم الإفتراضي وبالكاد تستطيع أجهزة الأمن العربية أن تتمكن من حماية الحدود الجغرافية فإذا بها تجد نفسها أمام الحدود الوبغرافية المائعة من دون موارد مناسبة وآليات عمل واضحة وأعداء مسلحين تكنولوجياً ومعرفياً وأقرب إلينا مما نتخيل. وفي الجهة المقابلة، برزت فرص جديدة ومثيرة لم تكن موجودة قبلاً، ومنها فرصة أن تكون سلة خدمات الحكومة جوّالة وقريبة من المواطن وفرصة الحكومة بالمشاركة الإجتماعية الأكثر فعاليّة منذ نشأتها وتواصلها مع محيطها ومواطنيها، وكذلك إمكانية الحكومة وبالاعتماد على الأجهزة الذكية المرتبطة بالإنترنت أن تعمل على تنظيم وإدارة الكثير من الخدمات العامة عن بعد وتوفير الوقت المستهلك في تجميع الداتا عن الأرض. إن الحكومة الذكية سوف يكون لها عيون تكنولوجية تراقب النشاط المعلوماتي في مختلف قطاعات المجتمع من أجل إضفاء المزيد من الفعاليّة والكفاءة على عملها.

twitter.com/ASPArabic
facebook.com/ASPArabic





